UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

FREE SPEECH COALITION, INC., MG PREMIUM LTD, MG FREESITES LTD, WEBGROUP CZECH REPUBLIC, A.S., NKL ASSOCIATES, S.R.O., SONESTA TECHNOLOGIES, S.R.O., SONESTA MEDIA, S.R.O., YELLOW PRODUCTION S.R.O., PAPER STREET MEDIA, LLC, NEPTUNE MEDIA, LLC, JANE DOE, MEDIAME SRL, MIDUS HOLDINGS, INC.,

Plaintiffs,

vs.

ANGELA COLMENERO, IN HER OFFICIAL CAPACITY AS INTERIM ATTORNEY GENERAL FOR THE STATE OF TEXAS,

Defendant.

Case No.: 1:23-cv-917

DECLARATION OF RICHARD L. SONNIER III IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED PRELIMINARY INJUNCTION

DECLARATION OF RICHARD L SONNIER III

I, Richard L Sonnier III, declare as follows:

1. I have been retained by Plaintiffs in the above captioned matter to provide technical expertise in the areas of Internet technologies and operations including age verification of users, content filtering, parental controls, family safe usage, the cost of implementing Internet technologies, the cost of operating Internet technologies, Internet privacy, Internet standards, cybersecurity, and Internet regulations.

2. My rate for time spent preparing this declaration and for the testimony in this matter is $350 per hour.

3. My compensation in no way depends on the outcome of this litigation or the testimony or opinions that I express.

I. BACKGROUND & EXPERIENCE

4. My qualifications as an expert witness can be found in Exhibit A, which includes my CV and a list of my publications and previous testimony.

II. SUMMARY AND SCOPE OF OPINIONS

5. In my opinion, Internet age verification as required by the State of Texas (and various other US state governments) has numerous problems; and Internet content filtering is a superior solution to achieve the apparent objectives of age verification.

III. MATERIALS CONSIDERED

6. In forming the opinions expressed in this declaration, I considered and relied on my education, experience, and knowledge of the relevant fields. I also reviewed and considered the materials listed in Exhibit B.

7. I reserve the right to rely on any other information, deposition testimony, trial testimony, documents, or materials that may be provided to me or that witnesses at trial rely on if called to testify about any aspect of this matter.

IV. INTERNET TECHNOLOGIES

8. To explain the Internet technologies, I will relate them by analogy to physical postal mail. However, like all analogies, this is imperfect. At the technical level, the operations

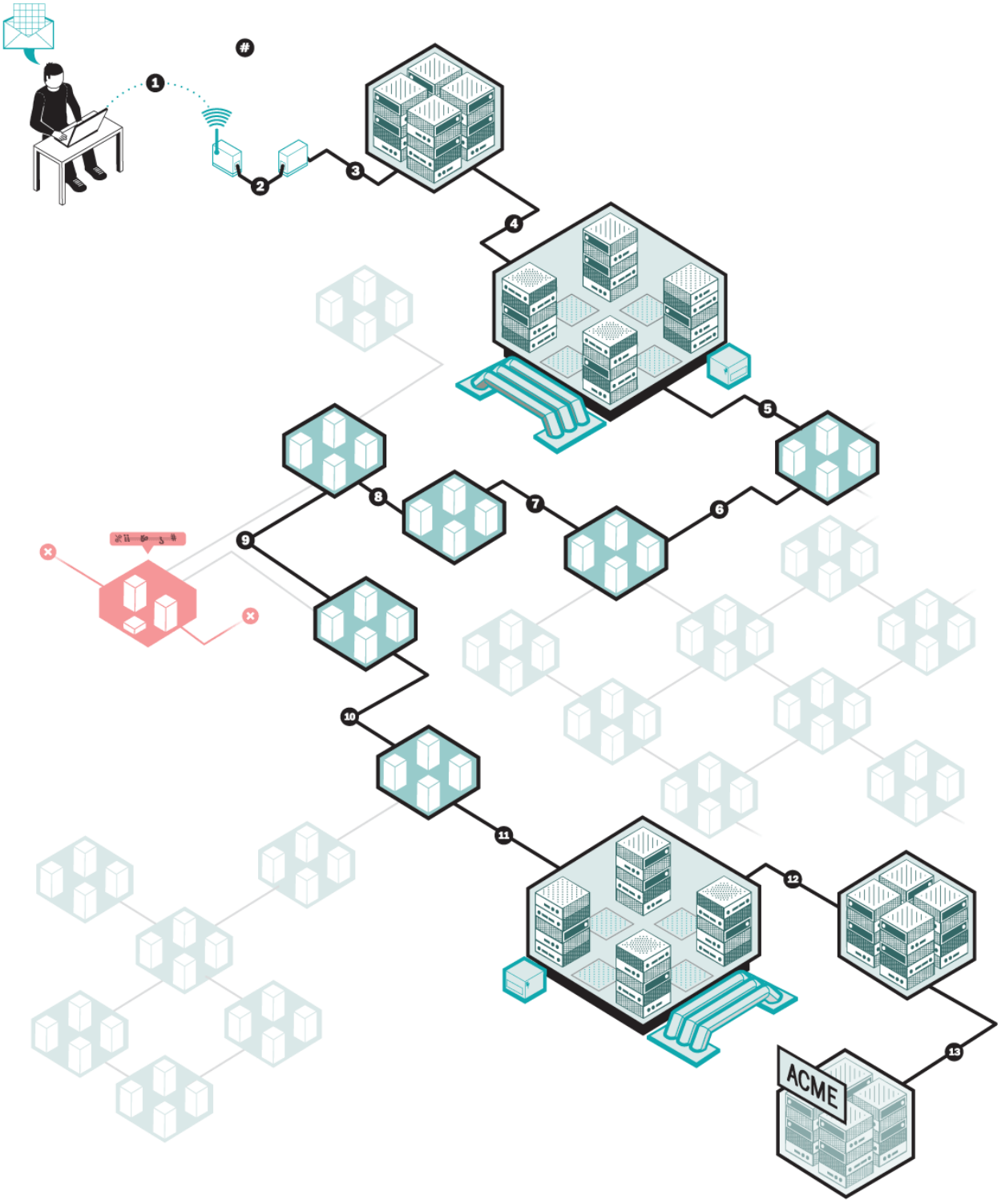
of the physical world—that is, items or products moving through time and space between producers and consumers—are fundamentally different from the movement of services or virtual products over the Internet. All too often parties apply physical world rules, regulations, and processes to Internet commerce.

9. Physical postal mail works as follows:

Steps	Internet Analogy
Write the letter	Create content
Insert the letter in the envelope	Wrap the content in a packet
Address the envelope	Address by putting the sender and recipient computer locations on the Internet into the packet
Hand off to the postal service	Insert the packet into the Internet
Route through the postal service network	Route through the Internet
Delivery to addressee	Deliver to the computer location of the recipient
Open the envelope	Open the packet on that computer
Extract the letter	Extract the content
Read the letter	Use the content e.g., display it on the computer screen
If needed, reply to the letter using the return address by repeating all steps from the top	If needed, use the sender's computer location to reply by repeating all steps from the top

10. To extend the analogy further, the routing of a packet through the Internet is like the routing of an envelope through the postal service network. The packet will go through several intermediate Internet locations before reaching the recipient's computer location. At each of these intermediate locations, the recipient's computer location will be read from the packet and used to determine the next location on the way to the recipient's computer location—just like the envelope goes from postal office to postal office on its way to the addressee. In both cases, this routing can be quite complex. For example, here is an illustration from the Washington Post, May 31, 2015, showing Internet routing (each numbered black circle indicates a step in the routing)[1]:

[1] https://www.washingtonpost.com/graphics/national/security-of-the-internet/bgp/



11. If you were sending a highly confidential letter, you might hire a representative, a proxy, near the addressee and place the addressed envelope into a secure box with a combination lock. Then you would address the secure box for delivery to your proxy, with instructions to

deliver it in person to the addressee. And you would provide the combination lock code to the addressee via a phone call, but not to your proxy. When the proxy delivers the secure box to the addressee, this ensures that no other parties except you and your addressee can read the letter and that it has not been altered. For the Internet, you can have the same assurance for your content by using encryption.

12. To understand how the Internet works, it helps to understand its history. The Internet was designed for the US Department of Defense to enable command and control communications within the military even in the event of a nuclear war that has destroyed the traditional centralized telephone and other communication systems. Thus, at its core the Internet is resilient in the face of damage. The Internet is designed to be highly adaptable. This makes the Internet resistant to traditional censorship and regulation. "[A]s Internet pioneer John Gilmore puts it, 'The Net [Internet] interprets censorship as damage and routes around it.'" *See* Exhibit C: the Time magazine article "First Nation in Cyberspace," Dec. 6, 1993.

V INTERNET AGE VERIFICATION

13. Internet age verification is a set of techniques to determine the age or likely age of a consumer interacting with a commercial website. The website could be selling products or services that require a minimum age, like tobacco products or online gambling; or the website could provide adult content, e.g., sexual material. Chelsea Jarvie and Karen Renaud presented an excellent summary of the current state of Internet age verification at the Dewald Roode Information Security Research Workshop, San Antonio, Texas in 2021, in their presentation and paper titled "Are you over 18? A Snapshot of Current Age Verification Mechanisms." *See* Exhibit D. Jarvie and Renaud examined 1119 papers from academic databases and the Internet to find 35 papers that were relevant to the Internet age verification between the years 2011 and 2021. Jarvie and Renaud determined from their review of the Internet age verification literature that such techniques should meet the following objectives: 1) Effective & Inclusive, 2) Affordable, 3) Privacy Preserving.

14. They further found Internet age verification techniques that require a copy of a government issued ID to be "highly privacy invasive." They also found assumptions that minors will not have access to credit cards or "their parents' identity documents" to be incorrect.

15. Jarvie and Renaud compiled a table of available commercial Internet age verification techniques:

Table 2: Age Verification Products (details based on website check in June 2021)

Solution	Checks	Price
WHAT YOU KNOW		
Renaud and Maguire [61]	Knowledge and ability to identify photos of historical figures	N/A
WHAT YOU ARE		
Yoti [92]	Picture (AI)	25p per verification
Verify my Age [80]	Video (AI)	45p per verification (eBay)
WHAT YOU HOLD		
Yoti [92]	Government ID Phone Number	25p per verification
Verify my Age [80]	Third Party Database Check Government ID Credit Card Check Phone Check	45p per verification
VeriMe [81]	Phone Number Check (if using debit card)	Unknown
AgeChecker [2]	Third Party Database Check Phone Number Check	$25 per month plus 50 cents per verified user
AgeChecked [1]	Driving Licence Phone Number Check Social Media Payment Card Address Search	Unknown
Trullioo [78]	Government ID Third Party Database Check	Unknown
Melissa [46]	Address Check	Unknown
Equifax [19]	Third Party Database Check	Unknown
Experian [20]	Third Party Database Check	Unknown
WHAT YOU HOLD & ARE		
AgeChecker [2]	Selfie with ID (AI)	$25 per month plus 50 cents per verified user
Jumio [37]	Selfie with ID (AI)	Unknown
Tencent [8]	ID Card + Facial Recognition	Unknown

16. Regarding the three objectives of Internet age verification vis-à-vis the available techniques, Jarvie and Renaud concluded:

> A range of solutions exist, as discussed in Sections 4.1 and 4.2. There are severe limitations in terms of efficacy. Where the solution is effective, it is almost always extremely privacy invasive. Where the solution is privacy preserving, it tends to be ineffective.
>
> Currently, the most utilised method for age verification is a tick

> box for the user to confirm they are over 18 (e.g., Figure 4). Other common methods include taking a photo of the user and using AI to determine the user's age. These are not infallible, as we show in Figure 6. Privacy invasive mechanisms dominate, including taking credit card details, requiring personal information to be provided to enable third-party database verification or having a phone number verified (e.g., Figure 5).
>
> Considering the challenges on each of the dimensions enumerated in Section 2.3, we see that the available solutions generally fail on at least one of the dimensions, with the majority invading privacy.

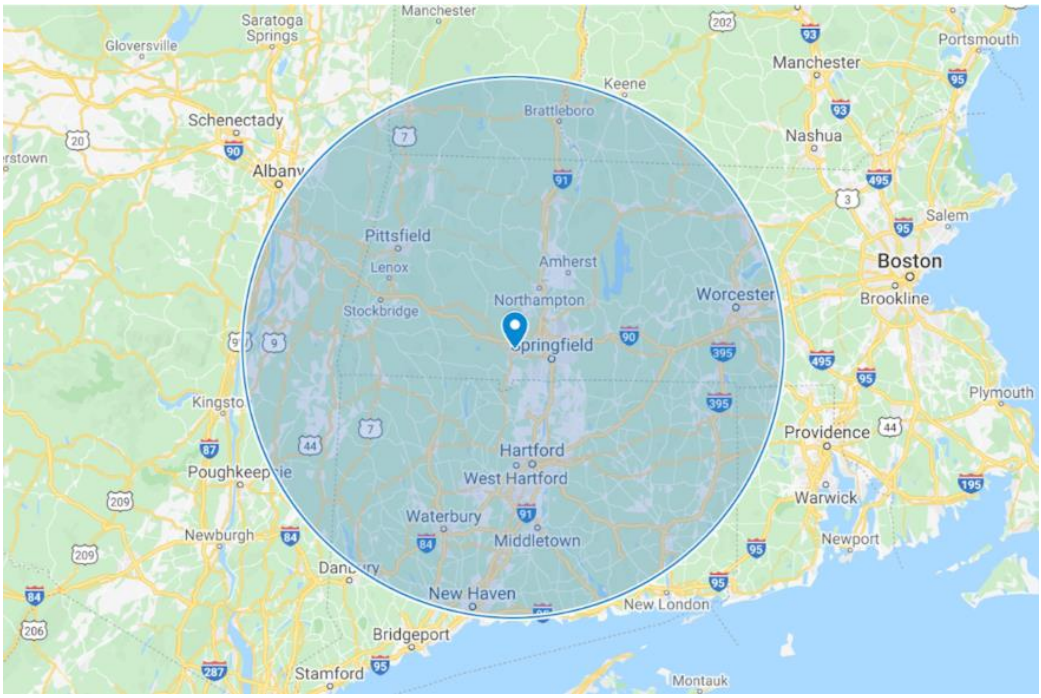
17. In my opinion, it makes sense that Jarvie and Renaud found that Internet age verification fails the key objectives. Due to the nature of current Internet technologies, Internet age verification is trying to solve the problem of limiting access to age restricted websites in the wrong place and with the wrong toolset.

VI ISSUES WITH INTERNET AGE VERIFICATION

18. The nature of the Internet (as discussed above) suggests that current Internet age verification technology will not work, and this is in fact the case. First, an Internet website cannot accurately and consistently determine the geographical location of its user. To apply the age restrictions for a particular state, a website must determine if the user is in that state. However, there is no mechanism to reliably do that. What is sometimes called the "geolocation" of the user is nothing of the sort; instead, it is the last known geolocation of the computer connecting to the website based on that computer's Internet address. Various service providers of geolocation information compile large databases of Internet addresses and their approximate or best guess geolocation in the world. In large part, these geolocation service providers rely on information reported by Internet Service Providers, registries of Internet addresses, as well as big data methods. MaxMind, Inc., one the major geolocation service providers, describes it this way:

> All of our IP geolocation data comes with an accuracy radius field. The actual geolocation of the IP address is likely within the circle with its center at the geolocation coordinates and a radius equal to the accuracy radius field. While the pin on the map might lead us to think that the IP address is close to the center of this circle, in reality we're defining a region in which the IP address is very likely to be.

Thus, the first step in applying the correct state age verification law rests on a guess of where the user "is very likely to be." MaxMind provides this example of an accuracy radius field:



So, an Internet website receives a connection from an IP address and asks MaxMind for its geolocation; and the website gets this circle from MaxMind with the assurance that the user's IP address is "very likely" in this circle. However, that circle includes parts of Connecticut, Vermont, Rhode Island, New Hampshire, Massachusetts, and New York. The website cannot apply the applicable state age verification law, if any, because it does not know in which state the user is located.

19. IP Location provides an Internet website that allows you to lookup the geolocation of an IP address in multiple services at the same time. For example, I disconnected my Verizon cell phone from my office Wi-Fi and then looked-up the IP address that Verizon assigned to my phone on the IP Location website. My cell phone's IP address was 174.203.0.3 and IP Location returned the following possible locations from the various geolocation providers: Beaumont, Texas; Houston, Texas; New York, New York; Baton Rouge, Louisiana; Ashburn, Virginia; Houston, Texas; Ashburn, Virginia; and Houston, Texas. At the time, my cell phone was in the zip code 77018 in which encompasses Houston, Texas. Thus, three of the eight geolocation services identified the correct city and state and one more identified the correct

state but was off by approximately 78 miles. However, the other four services failed to identify the correct city or state, with one missing my cell phone's location by approximately 1420 miles. IP Location explains that the accuracy of geolocation from IP addresses is the result of many factors.[2] IP Location cites a rough measure of geolocation accuracy based on the claims of the providers: the country of the IP address is accurate between 95% and 99%, the accuracy of the region or state of the IP address is between 55% and 80%, and the accuracy of the city of the IP address is between 50% and 75%. However, IP Location warns "the actual result may vary from provider to provider," and that the geolocations of cell phones may be less accurate than those for home computers. IP Location's estimate of accuracy matches with my test results where the city was accurate for 38% of the providers, the state was accurate for 50% of the providers, and the country was accurate for 100% of the providers.

20. The accuracy of the geolocation of IP addresses is limited by the nature of the Internet. A block of IP addresses is assigned to the Internet Service Provider (ISP) and that ISP has flexibility to assign each address to a user's device. Depending on the network technology of the ISP and the implementation choices they make, that block of addresses could be assigned to user's devices over a small geographic area or a very large one. Within those areas, any address can be dynamically assigned to many different user's devices over time. The IP address can easily, and often does, change each day. The geolocation providers compile the address blocks assigned to each ISP and then make determinations of likely geographic service area for that block. They then report the geolocation as the center of that service area and provide a confidence window for the entire area.

21. In the context of cell phones and cellular networks, the accuracy of geolocation can degrade quite a bit, because the large national carriers like Verizon have very large IP address blocks, which can be assigned over very large, multistate service areas or even the entire country. For example, I have traveled with a Verizon mobile hot-spot in a car from Virginia through Tennessee, Alabama, Georgia, Mississippi to Louisiana. The IP address assigned to the hot-spot rarely changed, despite my going in and out of the range of numerous cell phone

[2] https://www.iplocation.net/geolocation-accuracy

communication towers. During this trip, my geolocation was changing continuously but my IP address was not.

22. Another example of the issues with geolocation was reported by a Verizon cell phone user trying to listen to Philadelphia Phillies games over his cell phone. The user reports that sometimes his listening is blocked because although he is located in Delaware, which is in the designated market area for the Phillies games, his cell phone gets assigned an IP address located in York, PA, which is not. When this happens, the cell phone is blocked from playing the game audio.[3]

VII YOU CAN BE ANYWHERE YOU WANT TO BE

23. As I noted above, physical-world rules about where an individual is located don't apply to Internet commerce. Since the Internet fundamentally does not know where the user is in the world and, by design, does not care for its proper function, the user can appear to be pretty much anywhere in the world they would like to be. There are numerous mechanisms to achieve this: proxy servers, virtual private networks (VPNs), virtual desktops, remote desktop access, the Orion Router (TOR), and peer to peer networking or decentralized websites. Before going into the specifics of each of these technologies, I should point out they were all created to solve legitimate Internet problems dealing with security, privacy, and efficiency. They were not created to evade state law or facilitate criminal activity. Internet technologies are neutral, but Internet users vary. For example, TOR was created by researchers at the Center for High Assurance Computer Systems, Naval Research Laboratory, Washington; and, disclosed to the public in a January 28, 1999, paper. *See* Exhibit E. Its purpose was private communications over public networks like the Internet. Today, many security professionals consider TOR a security risk, the playground of hackers, and part of or a gateway to the dark web.

24. Going back to the postal email analogy described above, a proxy server is like using a private postal service for your mail. You don't give anyone your real address, instead you provide the private service's postal address, and the private service picks up your outbound

[3] https://community.verizon.com/t5/Other-Network-Discussions/How-are-IP-addresses-assigned-for-phones/td-p/1254931

mail and delivers any mail it receives for you. To the world, your real location is hidden by the private postal service. Similarly, a proxy server on the Internet will hide your computer's IP address from any website. Instead, the website will see the IP address of the proxy server. For example, ProxyScrape provides a list of free proxy servers, and faster and safer ones for a small fee. One of the free proxy servers was geolocated by MaxMind as "very likely to be" in Los Angeles, California, so a user in a state with restrictive laws could use it to fall under California law instead. ProxyScrape offers proxy servers in 129 countries around the world, so you can be almost anywhere you want to be.

25. Just like proxy servers, VPNs hide your actual IP address from the Internet website by presenting the IP address from the VPN instead. The major difference is that all the communication between your computer and the VPN is fully encrypted, which may not be true for a proxy server. Another difference is that some Internet activity may not work through a proxy server, whereas VPNs will support any type of Internet activity. Certain proxy servers are free. Similarly, VPNs, which are easy to set up, either come at no charge (such as Proton VPN), or at a minimal cost, such as ExpressVPN, which offers a free trial period of 30-days, charges $12.95 per month, and allows you to "be" in 94 countries. Furthermore, within the USA, you can choose to be in 15 different states. There are many competing VPN services, so if ExpressVPN does not support a chosen location, there is a good chance another service will. For example, if you want to be from Texas and ExpressVPN cannot support you, its competitor VyprVPN will. Another low-cost VPN service is offered by Mozilla Firefox[4] for $5 per month. It is called Mozilla VPN and offers IP addresses in 30 countries.[5] Furthermore, VPN services customarily offer free trial options, thus allowing users to switch from one free trial offer to another to avoid incurring charges.

26. Virtual desktops became widely used during the COVID-19 period when most companies had their employees work from home. Virtual desktops are analogous to your private postal service providing you direct access to a computer in their office where you can create and

[4] https://www.mozilla.org/en-US/firefox/

[5] https://www.mozilla.org/en-US/products/vpn/features/

print your mail and they will scan onto that computer any mail you receive. Thus, you can be anywhere, and connect to the private service computer over the Internet. The virtual desktop has a public address that any website you access from the virtual desktop will see. While widely used by businesses, virtual desktops are now offered to individuals and students at very low cost, similarly to VPNs. For example, Shells.com offers virtual desktops for $5 per month and is rated "extremely easy to use" by TechRadar.[6] Shells.com virtual desktops can be accessed from many devices, including PCs, smart phones, and tablets. Shells.com highlights a "Browser in the Cloud" solution that would certainly allow users to view adult content without restrictions.[7] Shells.com offers six locations outside Texas. Alternatively, Amazon WorkSpaces is a virtual desktop with many more features and costs as low as $7.25 per month, plus $0.19 per hour of active use. Amazon offers the service from approximately 15 locations around the world, so your website access would come from one of those locations.

27. Remote desktops are similar to virtual desktops. Both allow the user to securely connect to a remote computer, and the user's website access then appears to come from that remote computer's IP address. The differences are 1) the remote computer is your computer, or a computer controlled by you, 2) you must install the remote desktop access software both your computer and the remote computer, and 3) free versions of the software are available for personal use. For example, suppose you are a 17-year-old student at the University of Texas in Austin, TX, living in the dorms on campus with a laptop; but your home is in Boston, Massachusetts where you have a desktop PC. You can install the remote desktop access software on both computers and then use your laptop in Austin to connect to the desktop in Boston. Now, the you can access a website from the laptop in Texas while appearing to be in Massachusetts. One example of this type of software is TeamViewer, which is free for personal use.

28. TOR is another tool that permits users to conceal their true location. TOR is maintained by a non-profit corporation, the Tor Project, which creates the software, distributes it,

[6] https://www.techradar.com/best/virtual-desktop-services

[7] https://www.shells.com/l/en-US/browser-in-the-cloud

and supports it. TOR software is free. The TOR network consists of thousands of relays run by volunteers around the world. TOR will hide your computer's IP address, and the website will see the IP address of the last TOR relay instead. Unlike VPNs, TOR protects from "man in the middle" attacks. With a VPN, the VPN service is the man in the middle. If the VPN service is not trustworthy or is compromised by criminals or some government, then the VPN offers no security at all. TOR protects against this by using at least 3 relays on the path from your computer to the destination website where each relay knows the previous node and the next node in the path. TOR's objective is to work around censorship and government restrictions so it will allow a user to bypass them, e.g., age verification laws. TOR is like my postal letter analogy using a proxy and secure box, except TOR uses at least three proxies together with an equal number of secure boxes nested inside one another. TOR can even circumvent the Great Firewall: part of China's much stricter laws on Internet usage. For TOR to be effective, it needs to be easy to use. As Autumn Skerritt, a Software Engineer at Cisco/Duo, puts it:

> Tor needs a lot of users to create anonymity, if Tor was hard to use new users wouldn't adopt it so quickly. Because new users won't adopt it, Tor becomes less anonymous. By this reasoning, it is easy to see that usability isn't just a design choice of Tor but a security requirement to make Tor more secure.

To that end, the Tor Project makes it easy to use TOR by providing a custom web browser pre-configured to use it as a simple download. Once installed, you can browse via TOR. To be a TOR relay is also simple if you have a suitable server and Internet bandwidth. For example, on a Linux server, it takes just 7 steps.[8]

29. These Internet technologies can be combined to avoid age verification. For example, VPNs can be used in combination with all the others.

VIII PEER-TO-PEER NETWORKS

30. Peer-to-peer networking avoids age verification law in an entirely different way. With peer-to-peer networking, there is no website delivering adult content. At most, there is an indexing website that provides a list of the content available via the peer-to-peer network. The

[8] https://community.torproject.org/relay/setup/guard/centos-rhel/

network is a collection of computers that have some portion of the content. It is a form of file sharing that is decentralized. There is not one website server sharing the content, but rather an army of ordinary user computers providing portions of it. Thus, there is no website landing page on which required notices can be displayed or where age verification can be enforced. Instead, the website just provides peer-to-peer networking instructions to access the content on that network with a network client application, not a web browser. For example, a very popular peer-to-peer network is Torrents, which uses the BitTorrent protocol. The software is free, with faster and enhanced versions available for a fee.

31. In my opinion, if Internet age verification laws become more common, workarounds like peer-to-peer networking will become much more prevalent.[9]

VIII INTERNET CONTENT FILTERING

32. Internet content filtering is a superior alternative to Internet age verification. In fact, controlling access to adult content has been a high priority for Internet content filtering from the beginning, and remains in high demand by large enterprises. Thus, despite the rapid evolution of the Internet, Internet content filtering has kept up with the changes. Internet content filtering is a critical component of cyber security for any computer or device with Internet access, and has long included filtering of adult content. Therefore, it is not surprising that Internet content filtering works better than Internet age verification for restricting access to adult content by minors.

33. Internet content filtering can be implemented at many levels such as at the ISP, at the home router, or at the user device, to provide an in-depth defense against malicious or unwanted Internet content. There are thus many avenues to use to block adult content from reaching minors. Further, Internet content filtering is tunable. For example, many of my corporate clients block gambling and firearm websites, along with adult content, while many families allow gambling and firearm websites and block adult content only.

34. Internet content filtering is widely available at no additional cost with an Internet connection, in the Internet router or firewall, and built-in to the software of many computers and

[9] https://adultblog.io/best-porn-torrent-sites/

devices. More advanced content filtering can be purchased at various price points. Thus, Internet content filtering is available that fits most user needs and budgets.

35. Some of the latest Internet technologies, such as Domain Name System (DNS) filtering and artificial intelligence (AI), are being applied to Internet content filtering, thus improving accuracy. DNS is the phonebook of the Internet, where you can look up the address of any website or other Internet service. By examining the content of each website in DNS and then categorizing it, DNS filtering allows the user to block or allow websites based on their categories. This filtering is dynamic in that once the user blocks a category like adult content, the DNS filtering services constantly scans the Internet and updates that category with the latest websites. Uncategorized websites can be blocked as well, to address the fact that newly registered websites are the most common source of malware, viruses, and other malicious content. For example, DNSFilter, one commercial provider of DNS filtering, will upon receiving a request to access an uncategorized website from a user initiate a real-time scan of that website's content through its AI engine to classify and determine if it is in one of the allowed categories for the user.[10] Because of its large infrastructure and investment in technology, this can be done without disrupting the user's work, e.g. with very little time delay from the user's perspective. For families, Cisco Systems, one of the largest companies for Internet technologies, provides DNS filtering free of charge via its OpenDNS FamilyShield service.[11]

36. Internet content filtering is embedded in many Internet access routers. A recent list of them is available with reviews from Lifewire, a well-known website promoting easy to use technology.[12] The best overall router was the Synology RT2600ac Dual-Band Gigabit Wi-Fi Router, available from Amazon for $150. The Lifewire reviewers found the parental controls on this device to be easy to adjust, such that parents with multiple children can tune the filtering to

[10] https://help.dnsfilter.com/hc/en-us/articles/1500008108542-uncategorized-sites
[11] https://signup.opendns.com/familyshield/
[12] https://www.lifewire.com/best-parental-control-routers-4160776

age appropriate levels for each minor in the household as well as configure default filtering for the entire home network, including guests.

37. Microsoft provides parental controls in its products and offers the Microsoft Family Safety service in both free and paid versions.[13] The free version includes "Web and search filters" as well as "App and game filters."[14] Apps and games can be another avenue to adult content on the Internet that can be controlled through these parental control tools. Similarly, Apple offers parental controls with its products such as the iPad or iPhone that include the option: "Limit Adult Websites."[15]

38. There also are technical solutions to make Internet content filtering easy for busy parents or those who are not technology savvy, including to manage the filtering on different devices that may have different parental control capabilities. The industry has developed a solution for this in the form of combo applications often called "Parental Control Apps," which

[13] https://support.microsoft.com/en-us/account-billing/getting-started-with-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344

[14] https://www.microsoft.com/en-us/microsoft-365/family-safety?ocid=cmmy4tuo5qp

[15] https://support.apple.com/en-us/HT201304

provide the user with a single interface to manage Internet content filtering. Here is one list of such applications by Verywell Family[16]:

Compare the Best Parental Control Apps

Company	Pricing	iOS/ Android	Number of Devices	Screen Time
Qustodio *Most Comprehensive*	From $54.95/year (multiple plan options)	Both	1-15 (depending on the plan)	Yes
Google Family Link *Best Budget*	Free	Both	Unlimited	Yes
Bark *Best for Older Kids*	From $5/mo. (multiple plan options)	Both	Unlimited	Yes
Canopy *Best for Younger Kids*	From $7.99/mo. (multiple plan options)	Both	3-10 (depending on the plan)	Yes
Net Nanny *Best for Real-Time Monitoring*	From $39.99/year (multiple plan options)	Both	1-20 (depending on the plan)	Yes
FamilyTime *Best for Time Monitoring*	$13.99/month	Both	up to 15	Yes
Life360 *Best for Location Tracking*	From free to $24.99/mo. (multiple plan options)	Both	Unlimited	No

One aspect of parental control applications is that they monitor the Internet content access and keep a history of websites visited, often including snapshots for parental review. Monitoring allows the parents or guardians who supervise the minor's activities to calibrate their preferences

for protecting the minors, making a family-by-family, case-by-case determination according to the items of risk or that are concerning to them. One-size-fits-all-restrictions may not meet the needs within or across households.

39. Most of the Internet content filtering provided by these parental control applications is dynamic, in that parents select specific categories of websites to block. These applications will analyze each website and then the software will apply the category rules the parents have selected. For example, Qustodio says "Qustodio analyzes the content of each page each time it is visited. It then decides if the content is unsafe or suspicious, according to the rules you have set, and applies a category to that page. This process is continuously tested and improved."[17] Another example, Canopy, says "Our patented SafeSmart Internet Filter uses artificial intelligence to scan, detect, and eliminate explicit content on web browsers and many popular apps in milliseconds, before it reaches their screen" and specifies that it "makes real-time decisions about content, doesn't rely on an incomplete or outdated list of inappropriate sites."[18] Thus, these applications operate dynamically similar to DNSFilter as explained above. Additionally, Canopy works on all children's devices, including phones, tablets and computers, as does Qustodio.[19]

X INTERNET SEARCH ENGINES

40. Search engines, such as Bing.com, scan most Internet content so that users can search for it. Since search engines scan adult content and most users don't want such content in their results, search engines developed mechanisms to identify adult content and filter it out of their search results, depending on the level of "safe search" options a user selects. There are

[16] https://www.verywellfamily.com/best-parental-control-apps-4779963#toc-compare-the-best-parental-control-apps

[17] https://help.qustodio.com/hc/en-us/articles/360005216237-Qustodio-is-not-correctly-classifying-a-website

[18] https://canopy.us/parental-control-app-technology/

[19] https://www.qustodio.com/en/

many types of content that need to be identified and filtered out like malware, viruses, scams, frauds, and other malicious Internet content.

41. Many Internet search engines allow users to specifically search for images and videos and to easily change their level of "search safety." Thus, by simply turning off all "safe search" filters and performing a video search with the search terms "hot sex," the result I got is that Bing.com displays sexual material, i.e., adult content videos. Absent content filtering software, which typically forces the "safe search" filters of search engines into their most protective settings, any minor users would get adult content by simply running a search.

XII LACK OF BATTLE TESTED INTERNET AGE VERIFICATION CONSIDERING THE RISKS

42. Given that Internet age verification requires or at least recommends as a first or an enumerate choice the capturing of a government-issued ID, like a state driver's license or US passport, and that such documents are high value targets for many criminals, the risks to users of such age verification is very high. Internet age verification should be subjected to the same sort of extensive process as, for example, national encryption standards. There should be complete transparency of the algorithms, techniques and operating procedures including reference implementations suitable for testing by security researchers.

43. Considering the history of the SSL/TLS encryption network, the most widely used security on the Internet, shows 1) it takes the time to get security right, 2) major vulnerabilities are essentially inevitable, 3) it is a costly endeavor to maintain effective security. SSL 2.0 was widely deployed in 1995 to address the security needs of the Internet, only to be revised a year later as SSL 3.0 to address vulnerabilities in SSL 2.0. Then in 2014, a major security vulnerability, POODLE, was found in SSL 3.0, forcing an Internet-wide migration effort to TLS that was very costly to both providers and users. Millions and millions of devices had to be upgraded. Older devices require manual effort by technicians to upgrade firmware or software

and manually disable the badly broken SSL 3.0; in some cases, the devices could not be fixed and had to be replaced entirely.

XIV CONCLUSIONS

44. I conclude, as explained above, current Internet age verification technologies have little to no efficacy, including because they are easily circumvented by minors and carry significant risks to the privacy of personal information.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 1st day of August 2023 in Huston, Texas.

Richard L Sonnier III

RICHARD L SONNIER III

EXHIBIT A

Curriculum Vitae

Richard L Sonnier III

Houston, TX

PH: 281-445-4800

Email: rsonnier@nimbleservices.com

SUMMARY OF QUALIFICATIONS

I bring over 35 years of experience and skill to Nimble Services' customers who need cost effective computer systems and networks. I create solutions across a multitude of computer platforms and network technologies and focus on solutions with longevity based on industry standard technology.

Analyze and Design

- High performance computer infrastructures integrated with legacy systems
- High speed LANs/WANs/SANs and client/server architectures using Ethernet (10/100/1000) Switches, Routers, TCP/IP, Frame Relay, T1/T3, FDDI, Fibre Channel, TCP/IP, and the Internet
- Complex software systems including software architecture, performance tuning, source code analysis and migration from old to new platforms

Secure

- Computer security including audit preparation, audit remediation, penetration testing, policies and procedures

Integrate

- UNIX, NT, Solaris, HP-UX, AIX, IRIX, SCO, Digital UNIX, UNICOS, MPE/iX, MVS, Linux, and Windows networks into coherent company information system
- Standard and custom solutions with BMC ASA software: Patrol, BEST/1, SQL*Backtrack

Implement

- Computer systems management including policies, procedures, knowledge transfer, and products
- Network services: distributed backup, network printing, E-mail, security, universal file and data access, ORACLE, SQL Server, AFS, NFS, DFS, Samba, www, ftp, and high availability servers

Troubleshoot

- All aspects of complex networked systems focusing on increased performance and seamless ease of use

Develop

- Complex software systems including software architecture and design
- Custom system services and applications to provide complete computing environment in C, C++, C#, FORTRAN, Visual BASIC, Pascal, LISP, Korn, Perl, TCL/TK, SQL, NT Batch, Java, JavaScript, PowerShell, Python, Zig and Go.

Manage

- Complex software systems design and development projects
- Complex systems integration and management projects

BIOGRAPHY

I am the co-owner of the Nimble Services, Inc. based in Houston, Texas. I graduated from Louisiana State University in 1985 with a B.S. in Physics and second B.S. in Computer Science, and I have over 30 years experience designing technical computing solutions.

I began my professional career at Litton Industries supporting a US Navy contract creating a large database of warship design and support data. I was responsible for all aspect of the system: database, data storage, high-speed networking, imaging and scanning, and data visualization. I developed and implemented operational support systems and data converters. In my last assignment with Litton, I was the DB2 Database Administrator for a large business unit.

After leaving Litton, I moved to Houston, TX and took a contract position with Exxon Corporation. Over the next ten years, I worked on numerous data storage and migration projects including a custom HSM system that migrated data from Apollo and Sun workstations to a large IBM mainframe attached to a very large tape storage facility and a large AFS implementation that scaled from a few hundred Gigabytes to 4 Terabytes during my tenure. I designed, developed and implemented the backup system for Exxon's AFS site using up to 8 DLT tape jukeboxes. Additionally, I served on the evaluation team that extensively tested all the major enterprise RAID storage products of that time. Ultimately, Data General Clarrion systems were selected and I was instrumental in rolling out the new system to a capacity of 25 Terabytes. Also, I connected the Netscape web server to Exxon's AFS data via a custom security plug-in and implemented one of the first web search engines deployed in Exxon.

While contracting at Exxon, I joined a start-up company, Paranet, as its first employee. At Paranet I was a technology leader and advised many project teams. I managed the development of two commercial software products. One was a geophysical map data converter that was very successful. The other was a data backup system that was one of the first systems to support the new 8mm and 4mm tape stackers and jukeboxes. This backup system was sold to Exxon and used in production for several years. Additionally, I

developed a custom driver for EPOCH Systems' InfiniteStorage Architecture to allow data backup and archive of Apollo workstation data to EPOCH systems.

After leaving Paranet, I co-founded Net Partners, Inc. where I continued to work on data converters for geophysical data and worked on many other types of information technology projects. My last project at Net Partners was leading a team to develop a seismic data processing collaboration platform for a seismic processing vendor. The project allowed seismic data to be processed and interpreted remotely over the Internet with a web browser. I designed and implemented the entire data management subsystem including the relational database. Also, while at Net Partners, I specialized in computer system performance analysis and capacity planning. I completed many performance-troubleshooting projects often involving large ORACLE databases, and I trained BMC Software's class instructors on BEST/1, BMC's well-known performance and capacity planning tool.

After leaving Net Partners, I founded Nimble Services, Inc. where I continued to develop and lead cutting edge information technology projects including:

- Converting a Microsoft Access application into a web-based solution serving a community of global users for a major chemical company.
- Developing many web-based interfaces to legacy computer applications and databases running on mainframe or minicomputers.
- Scaling up web application infrastructure to support thousands of users using clusters of application and database servers with secure, redundant firewall front-end systems.
- Designing high performance computer networks.
- Migrating legacy IT applications and systems to modern web-based solutions.
- Redeveloping risk management software for insurance claims to use latest Windows technologies.

EXPERIENCE

IT Security: Access Control Systems and Methodology

- Designed and implemented numerous security schemes to meet client needs using user IDs, security groups and ACLs available in most operating systems.
- Audited access control systems and security at many sites.
- Implemented custom password complexity programs at several clients.
- Analyzed password strength using cryptographic analysis and brute force attacks.
- Engineered solutions to eliminate clear text passwords in applications and databases using security standards and custom programs to encrypt passwords.
- Extended applications like web servers to use advanced system security features like Kerberos Authentication and ACLs.
- Unified access control across the network by integrating Windows, UNIX and other computer security.

IT Security: Telecommunications and Network Security

- Performed security penetration test including Internet, WAN and LAN.

- Developed custom firewall solutions based on the Linux operation system.
- Secured Internet access with firewalls: FWTK, MS Proxy Server, Cisco PIX/ASA, CheckPoint, NetScreen, NetMax, SonicWall, Linksys, routers and other network security devices.
- Evaluated firewall effectiveness and reported on the results.
- Performed TCP/IP network performance tests.
- Analyzed security incidents at many companies including ExxonMobil, Global Marine and Universal Weather.

Business Continuity Planning and Disaster Recovery Planning

- Developed business continuity plan for UNIX systems at several clients
- Implemented failover solutions including clusters and data replication.
- Designed hot and cold backup sites for several clients including network, hardware, software and security aspects.

Security Management Practices

- Presented security best practices to CIO level executives and IT staff at several clients.
- Trained IT staff on security management and maintenance.
- Presented on computer security at conferences like Houston Business Expo and GHRUG.

Security Architecture and Models

- Created security audit scripts to maintain compliance.
- Implemented audit remediation to comply with corporate policies.
- Developed SOX audit policies and procedures.
- Developed tax compliance system to track corporate tax filings and compliance.
- Conducted numerous Technical Control Analysis Processes (TCAPs) on many IT products and services for ExxonMobil. TCAP is ExxonMobil's security evaluation and audit process to ensure all IT products and services comply with corporate standards and policies.
- Designed ExxonMobil's B2 level security environment for its exploration company covering systems, software, networks and security training.
- Audited security practices against business policies at several clients including ExxonMobil, Global Marine, and Challenger Mineral.

Legal Analysis

- Performed forensic analysis of many systems and provided expert reports for 8 or more legal cases dealing with theft of intellectual property, serving as expert witness in several cases.
- Provided expert analysis and reports for a software patent case. This expert witness analysis was cited by the Circuit Court of Appeals in a successful appeal of the case and instrumental in the favourable outcome for the client: http://www.cafc.uscourts.gov/opinions/06-1440.pdf

Application and Systems Development

- Developed application level network security solutions where remote systems were granted access to mainframe resources based on their physical IP address and two factor user authentication.

- Developed web-based application requiring SSL security.
- Converted a low security commercial web server farm to higher security farm located in a physically secure co-location facility and designed remediation solutions to fix 90% of the risk exposures.
- Developed a security framework to improve security of the web-based applications.
- Integrated, programmed and managed IBM Series/1 computers that linked the IBM mainframe with machine tools on the manufacturing floor.
- Integrated several manufacturing floor systems with HP 3000 mainframe and later HP-UX server including shop scheduling system, labor data collection system, and DNC machine tools.
- Designed and developed the operating system based on Linux for custom manufacturing floor terminals.
- Developed custom data communication protocols for communication between the HP 3000 mainframe and the manufacturing servers running over both Ethernet and RS-232 serial links with full redundancy, failover and failback.
- Developed support software for testing of Blue Sky's custom TDC for high end physics experiments (STAR TOF experiment of the Relativistic Heavy Ion Collider at Brookhaven National Laboratory) in LabWindows/CVI.
- Managed the development team for Blue Sky's follow-up software to support their TDC including recruiting the team, designing the software, and debugging it.
- Developed the device driver for Blue Sky's line of high performance waveform digitizers as well as some parts of the firmware and VHDL for the PCI-E interface.
- Analyzed patents on embedded systems in vehicles and how those systems form a distributed multiprocessor system via an open communication system.
- Analyzed the source code for numerous electronic control units (ECU's) found in Ford vehicles especially how they communicate over the CANbus to form a loosely connected distributed multiprocessor system.
- Analyzed the specification and schematics of the electronic components installed in Ford vehicles known commercially as Ford SYNC; and how those components are linked to other systems including Ford SYNC services.
- Inspected and tested various combination of Ford ECU's on vehicle bucks.
- Developed embedded system software for custom electronics.
- Developed Windows device drives for custom hardware.

IT Infrastructure

- Managed technical tools for support personnel.
- Enhanced sales with technical support and technical information.
- Improved customer service levels by increasing site efficiency.
- Developed Help Desk and Network Inventory service offerings.
- Developed an AFS backup system.
- Configured Internet mail gateway and MS Exchange to support SMTP mail for 400 Exchange users.
- Managed the corporate network of Suns, HPs, Macs and PCs.
- Implemented a command line interface to TCP/IP sockets for UNIX systems.

- Implemented a UNIX and PC integration project using PC/TCP.
- Developed a UNIX file archival system using TCP/IP.
- Designed LAN and WAN networks with 100's of nodes using TCP/IP, IPX, and SNA protocols.
- Configured NFS for Suns tied to Apollo networks.
- Administered an IBM DB2 relational database system on a 4381.
- Created relational databases in ORACLE on a VAX VMS system.
- Administered a 50 node Apollo network with over 100 users.
- Administered an Empress relational database system.
- Tested new CAD software.
- Supported Versatec and HP plotters.
- Supported Optigraphics system and scanner.
- Supported the Symix/Syteline ERP, engineering design systems, and the manufacturing floor electronic test equipment and the integration between them.
- Developed custom applications interfacing with the Laserfiche document management system.

Business Systems Development

- Implemented Compiere ERP on ORACLE 9 and 10.
- Developed an engineering drawing control system.
- Developed a multi-media web application providing audio, video and application windows to remote Internet users.
- Setup UltraSeek Internet search engine to index and search corporate information.
- Administrated SQL Server and Net Dynamics server for database oriented Web applications.
- Improved a backup product with 8mm tape support on DOMAIN/OS and AFS support for Suns.
- Managed a geophysical map converter development team and developed the core application framework for the product.
- Developed a user interface for a GeoShare converter product.
- Developed a converter for 3D manufacturing data between Computer Vision and Calma CAD/CAM systems.
- Managed a CAD installation project that installed 3 division networks.
- Designed and implemented GUIs in DOMAIN/Dialog, Open Dialogue, X11, and OSF/Motif.
- Implemented TCP/IP to SNA gateways.
- Developed an IOS type manager for backing up Apollo networks to an IBM mainframe.
- Developed a color raster formatter for a Versatec 3444 plotter.
- Developed a user support/problem tracking system.
- Introduced software engineering techniques into CAD project.
- Developed a custom IBM/RJE server.
- Developed a plot control/management system.
- Developed a generic mailbox communications package.

Performance and Monitoring

- Developed a network monitoring application that used audio recording and playback for messaging.
- Fixed ORACLE SQL*Net operations and performance.

- Analyzed X11 performance over Frame Relay network.
- Developed a UNIX system performance tool.
- Created and taught computer performance classes features BMC's BEST/1 product.
- Analyzed the performance of databases, networks, clients and applications providing recommendations to increase performance and resolve bottlenecks.

Conversions

- Converted UNIX web server to NT 4.0 and IIS.
- Ported an application from DOMAIN/OS to HP-UX.
- Converted data from numerous different systems to new formats.
- Developed an HP 3000 MPE emulation layer to port an entire suite of business applications from MPE to HP-UX.

EXPERT WITNESS CASES

Testifying

- ASCENSION DATA & ANALYTICS, LLC v. PAIRPREP, INC. d/b/a OPTICSML, SEAN M. LANNING, AND JOHN MICHAEL BROZENA
- UNITED STATES OF AMERICA v. RAMESH "SUNNY" BALWANI (Theranos COO)
- AllVoice Computing PLC v. Nuance Communications, Inc.
- AirGas, Aeriform v. IWS Gas and Supply
- JOHN C. MITCHELL, ALAN J. HEARD, STEVEN N. CORBETT, and NICHOLAS J. DANIEL v. DOUGLAS HOLT, MICHAEL K. DAVIS, and JOSEPH H. MIGLIETTA
- ALLVOICE DEVELOPMENTS US, LLC v. MICROSOFT CORPORATION

Consulting

- EAGLE HARBOR HOLDINGS, LLC, and MEDIUSTECH, LLC v. FORD MOTOR COMPANY
- WCS v. TMI
- OmmiLabs v. Core Lab
- POLYDYNE SOFTWARE INC. v. CELESTICA INTERNATIONAL, INC.

Forensics

- James Roll vs GCA Services Group
- Jacintoport vs former employees
- AET vs C5 Communications, Eric Smith, et al.
- US Quality Furniture of Services Inc. vs Furniture Works Inc.
- Sanitors Services Inc. vs Nathaniel B. Shaw
- BASEOPS INTERNATIONAL, INC. VS. EDUARDO HERNANDEZ, INTERNATIONAL TRIP PLANNING SERVICES LLC, INTERNATIONAL TRIP PLANNING, LLC and MGAS GLOBAL AVIATION SERVICES LLC
- Brad Randell
- Conix
- GAO

- Massage Envy Imperial Oaks
- Boulevard Reality/Sudhoff
- Beacon Medical v. Steve Sullivan
- PointServe (Mobi) v. IPX
- All Star Outdoors v. Mahindra (USA)
- Pipeline Trenchers LLC
- Trading Technologies International, Inc. Patent cases
- T & T Engineering Services, Inc. v. Axel Michael Sigmar, et al

EMPLOYMENT

- Nimble Services Inc., Founder, President & Senior Systems Analyst 2001-Present
- Net Partners, Inc., Co-founder, Senior Partner 1993-2001
- Paranet, Inc., Senior Systems Consultant 1991-1993
- Prime Computer, Inc., Systems Integration Consultant 1990-1991
- Exxon Company, USA Systems Analyst (contract) 1988-1990
- Litton Industries, Inc., Systems Programmer/Analyst 1986-1988

EDUCATION

- Louisiana State University, B.S. Computer Science 1985
- Louisiana State University, B.S. Physics 1985
- University of Southern Mississippi, Graduate courses: Relational Database Systems and Software Engineering 1987
- Tulane University A. B. Freeman School of Business, Master Certificate in Business Management 2005

CONTINUING EDUCATION

- BMC Patrol Administration/Implementation
- Microsoft Windows NT Programming
- Developing File Systems for Windows NT
- BEST/1 for UNIX
- BEST/1 for Distributed Systems SureStart Engagement Process
- FileNET Panagon Sys Admin on UNIX
- OSF DME Workshop
- OSF DCE Internals
- Tivoli Management Environment Advanced Developer
- Advanced Perl Programming
- Mach 3.0 MIG Programming
- Porting the Mach 3.0 OS
- OSF/1 Introduction
- Project Management

- Parallel Algorithms and Architectures for 3D Image Generation
- X-Windows and Open Dialogue Programming
- Network Computing System (NCS) Programming
- MVS/XA Introduction
- IBM Series/I CF Support
- IBM Series/I EDL Programming
- Calma Apollo DDM System Support
- Introduction to Hypertext and Hypermedia
- Architecting on AWS

PUBLICATIONS

- UNIX Review, "Spotlight on FDDI" October, 1992
- LISA IV, “TCL and Tk: Tools for the System Administrator” October, 1992

Houston Business Review, Cost Effective IT series of articles, 2004-2005

- Cost Effective IT
- Cost-Effective IT 100 Megabit Wireless
- Cost-Effective IT Are PCs Getting Easier To Use
- Cost-Effective IT Auditing
- Cost-Effective IT Cell Phone 2005
- Cost-Effective IT Cell Phone Applications
- Cost-Effective IT Compiere
- Cost-Effective IT Cost Savings
- Cost-Effective IT EBusiness
- Cost-Effective IT Easy To Use Software
- Cost-Effective IT For Marketing Your Business
- Cost-Effective IT Future Technology
- Cost-Effective IT Hardware Failures
- Cost-Effective IT Hardware Trends
- Cost-Effective IT High Speed Wireless
- Cost-Effective IT In Emergencies
- Cost-Effective IT Internet Future
- Cost-Effective IT Internet Security
- Cost-Effective IT Linux And Open Source 2005
- Cost-Effective IT Mozilla Thunderbird
- Cost-Effective IT Netscape Reborn
- Cost-Effective IT Network Storage
- Cost-Effective IT New Developments March 2004
- Cost-Effective IT New Sales Software
- Cost-Effective IT Nvu
- Cost-Effective IT Offshoring
- Cost-Effective IT Open Source Compiere

- Cost-Effective IT Photo No No
- Cost-Effective IT Planning
- Cost-Effective IT Planning For New Year
- Cost-Effective IT Policies Procedures
- Cost-Effective IT Security Part One
- Cost-Effective IT Security Part Three
- Cost-Effective IT Security Part Two
- Cost-Effective IT Service Oriented
- Cost-Effective IT Software Failures
- Cost-Effective IT Stopping SPAM
- Cost-Effective IT Successful Ventures
- Cost-Effective IT The Business Process
- Cost-Effective IT The Compiere Difference
- Cost-Effective IT The Compiere Difference NEXT
- Cost-Effective IT The Dark Side
- Cost-Effective IT Tough Decisions
- Cost-Effective IT User Failures
- Cost-Effective IT Web Applications
- Cost-Effective IT Web Based Training
- Cost-Effective IT Web Development and Dreamweaver
- Cost-Effective IT Web Forms
- Cost-Effective IT Wireless Networking
- Cost-Effective IT Wireless Inventory

OTHER SKILLS

- Houston Business Show on CNN 650 Radio, Periodic Appearances and Guest Host, 2004-2005

REFERENCES

Available upon request.

EXHIBIT B

List of Materials Considered

URLs

https://adultblog.io/best-porn-torrent-sites/

https://arstechnica.com/tech-policy/2023/01/no-porn-without-id-louisiana-law-forces-porn-sites-to-verify-users-ages/

https://avpassociation.com/standards-for-age-verification/

https://aws.amazon.com/workspaces/pricing/

https://blog.maxmind.com/2021/07/how-accurate-is-ip-geolocation/

https://btcpeers.com/top-5-adult-crypto-projects-an-overview/

https://canopy.us/2023/07/04/how-to-block-inappropriate-websites-adult-content/

https://canopy.us/parental-control-app-technology/

https://community.torproject.org/relay/relays-requirements/

https://community.torproject.org/relay/setup/guard/centos-rhel/

https://community.verizon.com/t5/Other-Network-Discussions/How-are-IP-addresses-assigned-for-phones/td-p/1254931

https://db.dcp.utah.gov/edu/filtering.html

https://developers.google.com/search/docs/crawling-indexing/safesearch

https://developers.yoti.com/digital-id/mobile-integration

https://developers.yoti.com/digital-id/security---data-protection

https://forum.dfinity.org/t/censorship-and-ip-liability-expectations/2953

https://forum.dfinity.org/t/lets-get-the-decentralized-porn-sites-up-and-going/13937

https://forum.dfinity.org/t/parler-on-the-ic/1811

https://geekflare.com/dns-content-filtering-software/

https://help.dnsfilter.com/hc/en-us/articles/1500008108542-uncategorized-sites

https://k9-web-protection.en.softonic.com/

https://lawallet.com/commercial-verification/

https://learnsafe.com/the-limitations-of-content-filtering/

https://proxyscrape.com/blog/does-tor-hide-your-ip

https://signup.opendns.com/familyshield/

https://skerritt.blog/how-does-tor-really-work/

https://suip.biz/?act=all-country-ip&province=Texas

https://support.apple.com/en-us/HT201304

https://support.microsoft.com/en-us/account-billing/filter-websites-and-searches-in-microsoft-edge-3034d91e-5efa-9fbe-1384-46009f087ccf

https://support.microsoft.com/en-us/account-billing/getting-started-with-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344

https://support.microsoft.com/en-us/microsoft-edge/learn-more-about-kids-mode-in-microsoft-edge-4bf0273c-1cbd-47a9-a8f3-895bc1f95bdd

https://support.torproject.org/about/
https://support.torproject.org/https/
https://tools.zvelo.com/
https://us.norton.com/blog/privacy/tor-vs-vpn
https://vpnoverview.com/internet-safety/secure-browsing/keep-your-children-safe-online/
https://www.accscheme.com/
https://www.agechecked.com/content/
https://www.agechecked.com/gambling/
https://www.allpasstrust.com/en
https://www.asacp.org/index.html?content=parental_guidelines
https://www.bark.us/learn/bark-home/
https://www.bittorrent.com/
https://www.digicert.com/blog/evolution-of-ssl
https://www.digitaltrends.com/computing/teens-top-tech-savvy-chart-adults-lag-behind/
https://www.expressvpn.com/?msclkid=3a857574b4e417c8912811b7f0460b68
https://www.google.com/safesearch
https://www.iplocation.net/geolocation-accuracy
https://www.iwf.org.uk/our-technology/our-services/url-list/
https://www.lifewire.com/best-parental-control-routers-4160776
https://www.lifewire.com/torrent-file-2622839
https://www.linkedin.com/in/brandonls/?ref=skerritt.blog&original_referer=https%3A%2F%2Fskerritt.blog%2Fstart-here%2F
https://www.microsoft.com/en-us/microsoft-365/family-safety?ocid=cmmy4tuo5qp
https://www.microsoft.com/en-us/photodna
https://www.mozilla.org/en-US/firefox/
https://www.mozilla.org/en-US/products/vpn/features/
https://www.opendns.com/home-internet-security/
https://www.pcmag.com/opinions/louisianas-new-porn-law-is-a-privacy-time-bomb
https://www.quora.com/Is-Tor-basically-the-same-as-software-that-hides-the-users-ip-address
https://www.rtalabel.org/
https://www.shells.com/l/en-US/
https://www.shells.com/l/en-US/browser-in-the-cloud
https://www.shells.com/l/en-US/network
https://www.shells.com/l/en-US/whyshells
https://www.spiceworks.com/it-security/network-security/articles/top-10-content-filtering-software-solutions/
https://www.star-telegram.com/news/local/article277034458.html
https://www.teamviewer.com/en/info/free-for-personal-use/
https://www.teamviewer.com/en-us/

https://www.techradar.com/best/virtual-desktop-services

https://www.techradar.com/reviews/shellscom

https://www.tomsguide.com/us/pictures-story/450-bittorrent-clients-list.html

https://www.torproject.org/about/history/

https://www.verywellfamily.com/best-parental-control-apps-4779963#toc-compare-the-best-parental-control-apps

https://www.washingtonpost.com/graphics/national/security-of-the-internet/bgp/

https://www.webroot.com/us/en/resources/tips-articles/safety-pornography

https://www.webtitan.com/https-content-filtering-solution/

https://www.webtitan.com/internet-content-filtering-solution/

https://www.wm.edu/offices/it/services/network/virtualdesktop/faqs/index.php

https://www.yoti.com/blog/our-approach-to-security-and-privacy/

https://www.yoti.com/privacy/

https://www.yoti.com/security/

https://yoti.my.site.com/yotisupport/s/article/What-information-does-Yoti-store-about-me

https://zvelo.com/harnessing-the-power-of-website-categorization/

https://ro.ecu.edu.au/theses/2409/

https://datatracker.ietf.org/doc/html/rfc8674

https://5rightsfoundation.com/static/2089-2021-with-disclaimer.pdf?_cchid=5de613a54088e9532e49ae45cca908b8

https://help.qustodio.com/hc/en-us/articles/360005216237-Qustodio-is-not-correctly-classifying-a-website

https://www.qustodio.com/en/

https://support.mozilla.org/en-US/kb/block-and-unblock-websites-parental-controls-firef?redirectslug=Parental+controls&redirectlocale=en-US#

Documents

- Declaration of Tony Allen, Case 2:23-cv-02123-SM-DPC Document 18-15 Filed 07/17/23 in the Eastern District of Louisiana.(18-15.pdf)
- Act of June 12, 2023, Ch. 676, ¶ 2 (H.B. 1181) Tex. Sess. Law Serv. (HB01181F.pdf)
- WHO LACKED PHOTO ID IN 2020?: An Exploration of the American National Election Studies (CDCE_VoteRiders_ANES2020Report_Spring2023.pdf)
- Internet Filtering and Adolescent Exposure to Online Sexual Material (Filtering tech article.pdf)
- Are you over 18? A Snapshot of Current Age Verification Mechanisms (AgeVerification.pdf)
- An investigation into the effifficacy of URL content fifiltering systems, Brett Ronald Turner, Edith Cowan University (https://ro.ecu.edu.au/theses/2409/)

- A Concise Study of Web Filtering (A Concise Study of Web Filtering.pdf)
- Yoti Facial Age Estimation White Paper Full version March 2023 (Yoti-Age-Estimation-White-Paper-March-2023.pdf)
- Onion Routing for Anonymous and Private Internet Connections (Onion Routing for Anonymous and Private (CACM-1999).pdf)
- The internet treats censorship as a malfunction and routes around it? A new media approach to the study of state internet censorship (Rogers_in_Parikka_Spam_book_optimized.pdf)
- First Nation in Cyberspace (First Nation in Cyberspace -- Printout -- TIME.pdf)
- The Security Impact of HTTPS Interception (interception-ndss17.pdf)
- Encryption, Privacy, & Data Protection: A Balancing Act (encryption-privacy-data-protection.pdf)
- Tor: The Second-Generation Onion Router (tor-design.pdf)
- Cryptopolitik and the Darknet (Cryptopolitik and the Darknet.pdf)
- ICRAfail A Lesson For the Future (ICRAfail.pdf)
- Reimagining Digital ID INSIGHT REPORT JUNE 2023 (WEF_Reimagining_Digital_ID_2023.pdf)
- IEEE Std 2089-2021 (https://5rightsfoundation.com/static/2089-2021-with-disclaimer.pdf?_cchid=5de613a54088e9532e49ae45cca908b8)

EXHIBIT C

TIME

Monday, Dec. 06, 1993

First Nation in Cyberspace

By Philip Elmer-Dewitt

Back in the mid-1960s, at the height of the cold war, the Department of Defense faced a tough question: How could orders be issued to the armed forces if the U.S. were ravaged by a nuclear assault? The communication hubs in place at the time -- the telephone switching offices and the radio and TV broadcast stations -- were not only vulnerable to attack, they would also probably be the first to go. The Pentagon needed a military command-and-control system that would continue to operate even if most of the phone lines were in tatters and the switches had melted down.

In 1964 a researcher at the Rand Corp. named Paul Baran came up with a bizarre solution to this Strangelovian puzzle. He designed a computer- communications network that had no hub, no central switching station, no governing authority, and that assumed that the links connecting any city to any other were totally unreliable. Baran's system was the antithesis of the orderly, efficient phone network; it was more like an electronic post office designed by a madman. In Baran's scheme, each message was cut into tiny strips and stuffed into electronic envelopes, called packets, each marked with the address of the sender and the intended receiver. The packets were then released like so much confetti into the web of interconnected computers, where they were tossed back and forth over high-speed wires in the general direction of their destination and reassembled when they finally got there. If any packets were missing or mangled (and it was assumed that some would be), it was no big deal; they were simply re-sent.

Baran's packet-switching network, as it came to be called, might have been a minor footnote in cold war history were it not for one contingency: it took root in the computers that began showing up in universities and government ^ research laboratories in the late 1960s and early 1970s and became, by a path as circuitous as one taken by those wayward packets, the technological underpinning of the Internet.

The Internet, for those who haven't been hanging out in cyberspace, reading the business pages or following Doonesbury, is the mother of all computer networks -- an anarchistic electronic freeway that has spread uncontrollably and now circles the globe. It is at once the shining archetype and the nightmare vision of the information highway that the Clinton Administration has been touting and that the telephone and cable-TV companies are racing to build. Much of what Bell Atlantic and Time Warner are planning to sell -- interactivity, two-way communications, multimedia info on demand -- the Internet already provides for free. And because of its cold war roots, the Internet has one quality that makes it a formidable competitor: you couldn't destroy it if you tried.

Nobody owns the Internet, and no single organization controls its use. In the mid-1980s the National Science

Foundation built the high-speed, long- distance data lines that form Internet's U.S. backbone. But the major costs of running the network are shared in a cooperative arrangement by its primary users: universities, national labs, high-tech corporations and foreign governments. Two years ago, the NSF lifted restrictions against commercial use of the Internet, and in September the White House announced a plan to make it the starting point for an even grander concept called the National Information Infrastructure.

Suddenly the Internet is the place to be. College students are queuing up outside computing centers to get online. Executives are ordering new business cards that show off their Internet addresses. Millions of people around the world are logging on to tap into libraries, call up satellite weather photos, download free computer programs and participate in discussion groups with everyone from lawyers to physicists to sadomasochists. Even the President and Vice President have their own Internet accounts (although they aren't very good at answering their mail). "It's the Internet boom," says network activist Mitch Kapor, who thinks the true sign that popular interest has reached critical mass came this summer when the New Yorker printed a cartoon showing two computer-savvy canines with the caption, "On the Internet, nobody knows you're a dog."

But the Internet is not ready for prime time. There are no TV Guides to sort % through the 5,000 discussion groups or the 2,500 electronic newsletters or the tens of thousands of computers with files to share. Instead of feeling surrounded by information, first-timers ("newbies" in the jargon of the Net) are likely to find themselves adrift in a borderless sea. Old-timers say the first wave of dizziness doesn't last long. "It's like driving a car with a clutch," says Thomas Lunzer, a network designer at SRI International, a California consulting firm. "Once you figure it out, you can drive all over the place."

But you must learn new languages (like UNIX), new forms of address (like president whitehouse.gov and new ways of expressing feeling (like those ubiquitous sideways smiley faces), and you must master a whole set of rules for how to behave, called netiquette. Rule No. 1: Don't ask dumb questions. In fact, don't ask any questions at all before you've read the FAQ (frequently asked questions) files. Otherwise you risk annoying a few hundred thousand people who may either yell at you (IN ALL CAPS!) or, worse still, ignore you.

All that is starting to change, however, as successive waves of netters demand, and eventually get, more user-friendly tools for navigating the Internet. In fact, anyone with a desktop computer and a modem connecting it to a phone line can now find ways into and around the network. "The Internet isn't just computer scientists talking to one another anymore," says Glee Willis, the engineering librarian at the University of Nevada at Reno and one of nearly 20,000 (mostly female) academic librarians who have joined the Internet in the past five years. "It's a family place. It's a place for perverts. It's everything rolled into one."

As traffic swells, the Internet is beginning to suffer the problems of any heavily traveled highway, including vandalism, break-ins and traffic jams. "It's like an amusement park that's so successful that there are long waits for the most popular rides," says David Farber, a professor of information science at the University of Pennsylvania and one of the network's original architects. And while most users wait patiently for the access and information they need, rogue hackers use stolen passwords to roam the network, exploring forbidden computers and reading other people's mail.

How big is the Internet? Part of its mystique is that nobody knows for sure. The only fact that can be measured precisely is the number of computers directly connected to it by high-speed links -- a figure that is updated ! periodically by sending a computer program crawling around like a Roto-Rooter, tallying the number of connections (last count: roughly 2 million). But that figure does not include military computers that for security reasons are invisible to other users, or the hundreds of people who may share a single Internet host. Nor does it include millions more who dial into the Internet through the growing number of commercial gateways, such as Panix and Netcom, which offer indirect telephone access for $10 to $20 a month. When all these users are taken into account, the total number of people around the world who can get into the Internet one way or another may be 20 million. "It's a large country," says Farber of the Internet population. "We ought to apply to the U.N. as the first nation in cyberspace."

That nation is about to get even bigger as the major commercial computer networks -- Prodigy, CompuServe, America Online, GEnie and Delphi Internet Service -- begin to dismantle the walls that have separated their private operations from the public Internet. The success of the Internet is a matter of frustration to the owners of the commercial networks, who have tried all sorts of marketing tricks and still count fewer than 5 million subscribers among them. Most commercial networks now allow electronic mail to pass between their services and the Internet. Delphi, which was purchased by Rupert Murdoch's News Corp. in September, began providing its customers full Internet access last summer. America Online (which publishes an electronic version of Time) is scheduled to begin offering limited Internet services later this month.

People who use these new entry points into the Net may be in for a shock. Unlike the family-oriented commercial services, which censor messages they find offensive, the Internet imposes no restrictions. Anybody can start a discussion on any topic and say anything. There have been sporadic attempts by local network managers to crack down on the raunchier discussion groups, but as Internet pioneer John Gilmore puts it, "The Net interprets censorship as damage and routes around it."

The casual visitor to the newsgroups on the Usenet (a bulletin-board system that began as a competitor to the Internet but has been largely subsumed by it) will discover discussion groups labeled, according to the Net's idiosyncratic cataloging system, alt.sex.masturbation, alt.sex.bondage and alt.sex.fetish.feet. On Internet Relay Chat, a global 24-hour-a-day message board, one can stumble upon imaginary orgies played out with one-line typed commands ("Now I'm taking off your shirt . . ."). In alt.binaries.pictures.erotica, a user can peek at snapshots that would make a sailor blush.

But those who focus on the Internet's sexual content risk missing the point. For every sexually oriented discussion group there are hundreds on tamer and often more substantial topics ranging from bungee jumping to particle physics. Last week Virginia college student Chris Glover responded to a distressed message from a suicidal undergraduate in Denver. After two hours of messages back and forth, Glover was able to pinpoint the woman's location and call for help.

With all this variety, Internet users are unimpressed by television's promise of a 500-channel future. The Internet already delivers 10,000 channels, and the only obstacle that prevents it from carrying live TV pictures

is the bandwidth (or carrying capacity) of the data lines. Some video clips -- and at least one full-length video movie -- are already available on the network. And last spring, writer Carl Malamud began using the Internet to distribute a weekly "radio" interview show called Geek of the Week. Malamud is undeterred by the fact that it takes a computer about an hour over a high- speed modem to capture the 30 minutes of sound that a $10 radio can pick up instantly for free. But bandwidth capacity has nowhere to go but up, says Malamud, and its cost will only go down.

The Internet, however, will have to go through some radical changes before it can join the world of commerce. Subsidized for so long by the Federal Government, its culture is not geared to normal business activities. It does not take kindly to unsolicited advertisements; use electronic mail to promote your product and you are likely to be inundated with hate mail directed not only at you personally but also at your supervisor, your suppliers and your customers as well. "It's a perfect Marxist state, where almost nobody does any business," says Farber. "But at some point that will have to change."

The change has already begun. NSF's contribution now represents about 10% of the total cost of the network, and the agency is scheduled to start phasing out its support next April, removing at the same time what few restrictions still remain against commercial activity. According to Tim O'Reilly, president of O'Reilly & Associates, a publisher experimenting with advertiser-supported ^ Internet magazines, the system could evolve in one of two ways: either entrepreneurs will manage to set up shop on a free-market version of the Internet, or some consortium will take the whole thing over and turn it into a giant CompuServe. "That's an outcome," O'Reilly says, "that would effectively destroy the Internet as we know it."

As the traffic builds and the billboards go up, some Internet veterans are mourning the old electronic freeway. "I feel kind of sad about it," says Denise Caruso, editorial director of Friday Holdings, a publisher specializing in new media. "It was such a dynamic, pulsing thing. I wonder whether we shouldn't have left it alone." Others see the period of uncertainty ahead as a rare opportunity for citizens to shape their own technological destiny. "We need . . . a firm idea of the kind of media environment we would like to see in the future," warns Howard Rheingold in his new book, The Virtual Community. While it may be difficult for communities as diverse as those on the Internet to set their own agenda, it seems increasingly likely that if they don't, someone else will do it for them.

EXHIBIT D

Are you over 18?

A Snapshot of Current Age Verification Mechanisms

Chelsea Jarvie[1]
Karen Renaud[1,2,3]

[1]University of Strathclyde, Glasgow, UK
[2]Rhodes University, Grahamstown, South Africa
[3]University of South Africa, Pretoria, South Africa

karen.renaud@strath.ac.uk (Corresponding Author)

Proceedings of 2021 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, San Antonio, Texas, USA

ARE YOU OVER 18? A SNAPSHOT OF CURRENT AGE VERIFICATION MECHANISMS

Chelsea Jarvie[1], **Karen Renaud**[1,2,3]
[1]University of Strathclyde, Glasgow, UK
[2]Rhodes University, Grahamstown, Pretoria, South Africa
[3]University of South Africa, South Africa
chelsea.jarvie@strath.ac.uk, karen.renaud@strath.ac.uk

ABSTRACT

There are many online spaces that children should not enter to shield them from adult content, services and products. Age verification mechanisms are used to bar entry to minors. We examine the arguments for and against their use, and propose three dimensions that these kinds of mechanisms ought to judged by: (1) effectiveness & inclusivity, (2) affordability, and (3) privacy preservation. We used a systematic literature review to provide a snapshot of age verification practice in the research literature and commercial arena. We found a wide range of age verification mechanisms, ranging from "verification theatre" (box checking to confirm adulthood) to those that verify age by confirming identity. The latter elicit significant security and privacy concerns while the former clearly constitute no obstacle at all. Some mechanisms use facial biometrics to estimate age (for a fee), but the costs can easily become prohibitive for small businesses. We suggest directions for future research into solutions that can provide a more effective and affordable solution, which crucially also respect the privacy of users.

1 Introduction

Online safety for children is a mounting concern with more services for children, including education, being delivered online. One in three Internet users were children in 2015 [43], and during the pandemic era this percentage has surely increased with children spending far more time online since the beginning of the pandemic [24, 76].

Professor Byron [11] explains that online harms to children can be categorised into one of the three C's: (1) Content, (2) Conduct and (3) Contact.

Proceedings of 2021 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, San Antonio, Texas, USA

With respect to *content*, a report published in 2016, by the National Society for the Prevention of Cruelty to Children (NSPCC), The Children's Commission and Middlesex University highlighted long-term concerns related to children's development if exposed to adult content online [45].

With respect to *conduct*, Thompson [75] explains how teens can engage in risky conduct online, to their detriment. Sexting, too, is a rising trend [70], with possible tragic consequences [26]. Children are also increasingly exposed to online abuse or cyber bullying [52].

With respect to *contact*, there is an obvious need to protect children from online predators [88, 52].

Given that the online environment is beset with dangers to underage users, there is a growing need and demand for effective online age verification methods to protect children from viewing inappropriate content and to protect vendors from inadvertently selling adult products to minors, and facing legal consequences. Although there are robust physical controls to prevent children from accessing offline adult content or purchasing adult products, such as alcohol and tobacco, equivalent online controls might well still be immature and ineffective.

Different countries impose a range of legal age restrictions for 'adult' activities. For example, in the UK, you have to be 18 to drink alcohol, but in the USA. drinkers have to be 21[1]. The legal age for smoking also ranges from 16 (Zambia) to 18 (most of the world) to 21 (USA)[2].

The *conduct* and *contact* risks are best managed by non-technical mentoring and monitoring measures implemented by parents and teachers [62]. With respect to *content*, there is a distinct possibility that children might access adult-only content [25, 27], and reliable age verification mechanisms could prevent this.

Perlroth [57] explains that while it may seem a simple matter to verify the age of Internet users, it is actually very challenging to do this accurately. The last review of the available online age verification mechanisms was published in 2015 [61]. Given that five years have passed, we performed a systematic literature review to assess the state of play related to age verification. We surveyed the research and grey literature to reveal the full range of online age verification mechanisms. We discovered that age verification practice ranges from non-existent or light touch (checkbox to confirm age) to highly privacy invasive. There exists a substantial gap for an effective, affordable and privacy-preserving online age verification solution [61].

In Section 2, we review arguments for and against the use of age verification mechanisms, and suggest three dimensions that age verification mechanisms should possess. In Section 3, we detail the research methodology. Section 4 reports on the results of the analysis. Section 5 suggests future research, with Section 6 discussing, reflecting and acknowledging limitations. Section 7 concludes.

[1] `https://en.wikipedia.org/wiki/Legal_drinking_age`
[2] `https://en.wikipedia.org/wiki/Smoking_age`

2 Background

The UK Government's efforts to tackle the issue of children accessing adult content started with the Digital Economy Bill which received Royal Assent in 2017, making it the Digital Economy Act 2017 [28]. Part 3 of the Act focused on Age Verification for online pornography and measures were due to come into force from 15th July 2019. However, it was delayed and the act subsequently dropped in 2019, with the Government promising that other measures would be put in place [6].

In 2021, the UK Government released a new bill, The Online Safety Bill, which has no reference to online age verification for pornography sites [30]. This came as a surprise to children's safety groups and the commercial pornography industry who had been expecting and preparing for an age verification requirement [6]. The Government has come under fire from groups supporting age verification for access to adult content and recently lawyers began proceedings against the UK Government, claiming they have failed to stop children watching online pornography [72].

The oft-mentioned justification for age verification is to control access to online pornography [29, 74]. However, there remains a gap when it comes to online sales of alcohol and tobacco products worldwide. In a recent survey, Gaiha *et al.* found that more youths had moved to buying e-cigarette products online while shops were closed during the COVID-19 pandemic in the USA. Over a quarter were not asked to verify their age [25].

In a study by Wood [89] into youths purchasing e-cigarette products online in Australia, he found that 50% of vendors audited had no age verification process, and the remaining 50% required the user to confirm they were over 18 or input their age or date of birth. Similarly, Williams *et al.* [87] investigated online alcohol sales in the USA. They reported that only 39% of attempted online transactions by minors failed due to age verification mechanisms detecting them. A similar study by Colbert *et al.* [12] found that in Australia, of the alcohol vendors chosen, ineffective online age verification methods were used. 49% asked the users for their dates of birth and 27% utilised a tick box method.

Schiff *et al.* [67] found that in of the youths surveyed in Los Angeles, California, few experienced age verification barriers when trying to purchase e-cigarette products online. When it came to verifying the minors age on delivery of the product, Schiff *et al.* discovered that minors were circumventing the control by having their tobacco products delivered to an older friends house.

Age verification for online sales is a global issue and in 2021, the UK Government published a call for proposals for innovators to develop a way to fulfil the requirement for online age verification on alcohol sales, given that they have to comply with the Licensing Act 2003 [31].

In addition to the work being done by the UK Government, in 2020 the Information Commissioner's Office published the Children's Code [54]. The code contains 15 standards that must be complied with when designing online services that are likely to be accessed by children under the age of 18. It is worth noting that the code still applies to online services that may not be aimed at children and one of the standards concerns age assurance [54].

Social media services are significantly used by children with most sites requiring users to be at least 13 years of age [79] but age verification has proved a challenge. Consider TikTok, which in recent years has tried a range of methods. Some have been privacy invasive and others light touch and ineffective. In 2019, TikTok made multiple changes after violating the Children's Online Privacy Protection Act (COPPA), which resulted in many accounts which they believed belonged to underage users being blocked or deleted. Customers had to send a copy of their government ID to get their account back [17]. In January 2021, TikTok came under fire again and was ordered by the country's data protection agency to recheck the age of every user in Italy [71]. To achieve this, TikTok asked customers to re-enter their date of birth, and anyone who was under 13 years of age was removed from the app. This is an easy verification process to circumvent and significantly different to the approach taken in 2019. This demonstrates, once again, the need across multiple industries for effective, inclusive, affordable and privacy-preserving online age verification.

We first present the arguments *for* (Section 2.1) and *against* (Section 2.2) the deployment of online age verification mechanisms. We then suggest three dimensions that such mechanisms ought to possess (Section 2.3).

2.1 Arguments *for* age verification

The 2016 study by the NSPCC, The Children's Commission and Middlesex University found that by age 16, 65% of children had seen online pornography and that a higher number of boys than girls wanted to emulate what they had seen. This, in turn, made girls feel more worried about the impact pornography had on boys' attitudes to sex and relationships [45, 14]. Adolescents who access inappropriate adult content can have their perceptions of women permanently skewed [58] and experience negative emotional, psychological, and physical health outcomes [58, 60]. Moreover, two murders by a British 15 year old were attributed at least partly to his addiction to violent pornography [51].

Parents are concerned [55] and engage in a number of strategies to protect their children [53], but their influence is limited when children access the Internet from public WiFi and devices that their parents cannot control.

2.2 Arguments *against* age verification

Similar to Yar [91], Blake [7] is sceptical of introducing age verification for pornography sites, believing that this control will do more harm than good. Blake argues that statistics used by the UK Government related to online pornography causing harm to children is "cherrypicked". Blake states that there is no evidence that young people are harmed by seeing sexual images and that the main under-18 users of pornography are 16 and 17 year-old's who are above the age of sexual consent anyway. Introducing age verification, Blake believes, may actually expose children to a greater risk because they might turn to the dark web to circumvent the restrictions to access these services, and be at much greater risk in this completely unregulated domain.

2.3 Age Verification Solution Dimensions

The previous two sections presented arguments both for and against the use of age verification mechanisms to control access to adult-only online spaces. The arguments *for* their use appear more compelling than those of the detractors,

especially since governments might well mandate their use in the future [6]. If we *do* develop age verification solutions, what should their characteristics be?

Based on the literature, the ideal age verification mechanism should demonstrate the following dimensions (Figure 1):

(1) Effective & Inclusive: No tool will be infallible, but the probability with which a mechanism is able to identify children should be commensurate with the sensitivity of the content and the damage such access can do to children. This can prevent children from being harmed by inappropriate content. Moreover, a solution should not exclude any population group either due to minority status or limited financial resources. This aligns with the ISO accessibility standard [36], which aims at "*making products, systems, services, environments and facilities more accessible to more people in more diverse contexts of use*". We combine effectiveness with inclusivity because a these two aspects are inter-dependent.

(2) Affordable: In other domains, there is a strong link between affordability and adoption [68, 42, 69]. Hence, if governments mandate age verification for online vendors selling adult products, or providing adult content, it is essential for such mechanisms to be affordable, even for small businesses. Paying per transaction is likely to reduce small businesses' already small profit margins.

(3) Privacy Preserving: Renaud and Maguire [61] argue that age verification ought not to collect any personally identifiable information, to ensure that people are not blackmailed or sextorted by unscrupulous vendors. The Ashley Madison case amply demonstrates the consequences if such sensitive information leaks [3].

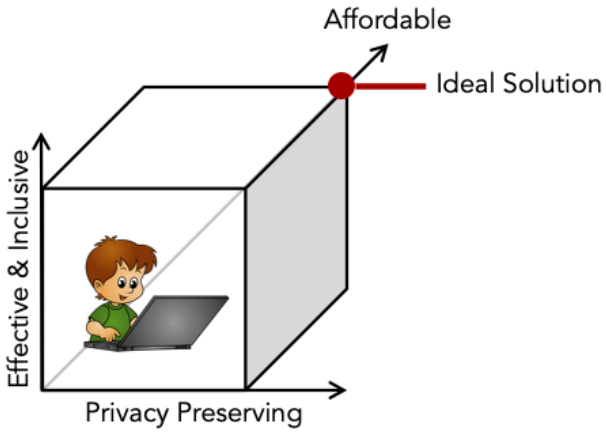


Figure 1: Age Verification Mechanism Dimensions

3 Research Methodology

3.1 Research Questions

The aim of this paper is to explore the current academic and industry position regarding online age verification, and to suggest directions for future innovative research in this space. This paper will explore the following research questions, which will inform the analysis process:

Research Question 1 (RQ1): *To what extent do online age verification solutions exhibit the three primary dimensions enumerated in Section 2.3?*

Research Question 2 (RQ2): *What other mechanisms could potentially be used to effect age verification?*

3.2 Systematic Literature Review

A systematic literature review was carried out to ascertain the extent to which current research could answer the two research questions posed in this paper. Our aim, in doing this research, was to reveal the state of play (RQ1) but also to determine whether the growing area of body language based deception detection [34, 64, 32] was, or could be, used to support online age verification (RQ2).

A variety of databases were used to gather relevant research including; Scopus, EBSCO, Web of Science and ProQuest, in addition to Google search engine for grey literature. Material was collected for the years between 2011 and 2021. Finally, we used an Artificial Intelligence (AI) powered tool called IRIS.AI to find any additional texts that may have been missed in previous searches. The methodology used is the approach proposed by [40] and is depicted in Figure 2.

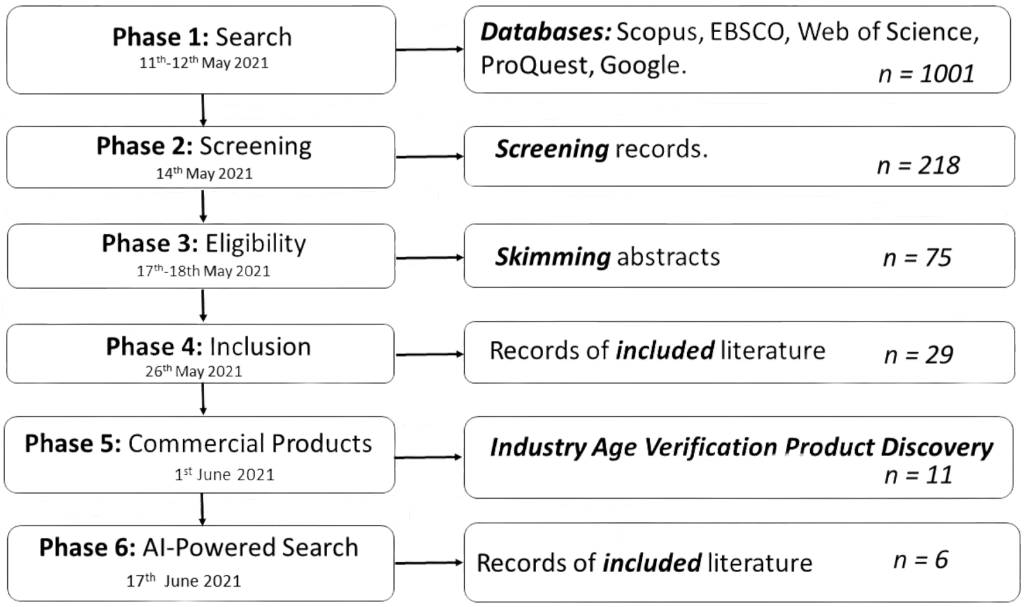


Figure 2: PRISMA of Systematic Literature Review [40]

Phase 1 - Identification: A total of 1001 resources were found from the databases listed using the keywords: "Cyber safety" or "online safety" and "children", "online age verification", "machine learning" and "lie detection", "online" AND "deception detection" AND "body language".

Phase 2 - Screening: After initial screening, it was found that 78% of the results were not relevant due to being out of scope or context. There were a considerable number of papers rejected regarding teaching children how to be safe online, cyber bullying and parental controls as these topics are not within the scope of this project. Similarly, where deception detection was based on physical measurements, papers were rejected.

Phase 3 - Eligibility: After reviewing the abstracts of the remaining 218 papers, 75 were retained.

Phase 4 - Inclusion: The remaining papers were fully structured and reviewed. The final review process eliminated all but 29 papers.

Phase 5 - Commercial Products: An extensive search was carried out using a search engine and the Keywords 'online age verification for businesses','online age verification' to identify as many commercial products as possible.

Phase 6 - AI-Powered Search: We finalised our search by using an AI powered tool called IRIS.AI. We provided it with the abstract for this paper, as well as the title: '*Age Verification Deception Detection*'. It returned 118 papers, with a graph as shown in Figure 3. We worked through each paper returned by this search to identify its relevance. A total of 6 papers were added to our original corpus. Table 1 provides the tallies of papers found in each database.

Table 1: Databases and numbers of papers found

Database	# Papers	After Exclusion
EBSCO	36	0
Scopus	224	15
Web of Science	9	0
ProQuest	732	14
IRIS.AI	118	6
Total Analysed	1119	35

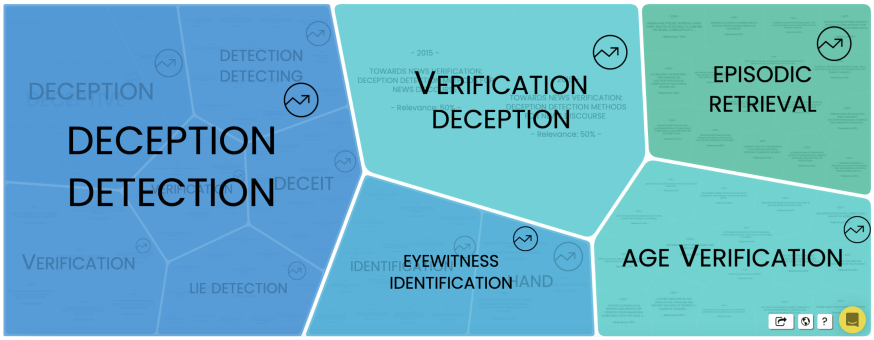


Figure 3: Result of AI-Powered Search

4 Findings

4.1 Current Processes

Although there is a push for effective online age verification, and online age verification solutions *do* exist, they vary significantly from "verification theatre" (check this box to confirm you're over 18) to highly privacy invasive (provide a copy of your passport).

Williams *et al.* [86] found the most common age verification methods used by online tobacco vendors was a checkbox asking the online user to confirm they were over 18; only accepting credit card payments, or telling them that by submitting an order, the user is implicitly verifying they were over 18. Similar methods were used by online alcohol vendors [87, 84, 12]. Moreover, Williams *et al.* identified issues throughout the adult product supply chain. Delivery companies were found to leave alcohol and tobacco packages unattended or gave them to youths without verifying ID [85, 12].

A small study by Williams *et al.* [85] revealed that, of 10 minors who tried to buy e-cigarettes online, none failed due to a working age verification process. In fact, they found that 46% of vendors used a tick box to confirm adulthood, 19% had no age verification at all and the final 35% had a strategy which failed in its core purpose in this study. In a larger study into alcohol sales carried out by Williams *et al.* into 100 alcohol orders placed by youths, only 39 failed due to age verification, with 51% of vendors having a tick box and 41% deploying no age verification solution [87]. A similar study by Colbert *et al.* [12] found that selected Australian alcohol vendors, 49% asked for a date of birth and 27% utilised the tick box method.

In summary, the most common age verification process demonstrated in these studies is the tick box, which cannot possibly be effective in preventing youths buying or accessing adult products and services. This method is essentially "verification theatre" (Figure 4). The only consideration recommending it is that it is privacy preserving. However, the balance between effective age verification and privacy is not achieved by using a tick box mechanism. Google's age verification mechanism, as shown in Figure 5, demonstrates an underlying assumption that: (1) children cannot get hold of credit cards, and (2) children cannot gain access to their parents' identity documents. Both of these are unfounded.

4.2 Commercial Products

Preventing children from accessing adult products, services and content online is a challenge which is highly debated politically and comes with a huge host of technical challenges. There is a small selection of commercial age verification solutions that vendors can pay for.

The available commercial products utilise a variety of methods to verify a user's age. The predominant methods use database checks or photos of the user that use AI to determine whether the user is underage or not.

Yoti uses AI to determine the user's age from a picture and also offer a digital ID scheme whereby a user uploads a government document and is provided with a QR code which can be used by vendors to prove ID. Yoti's age

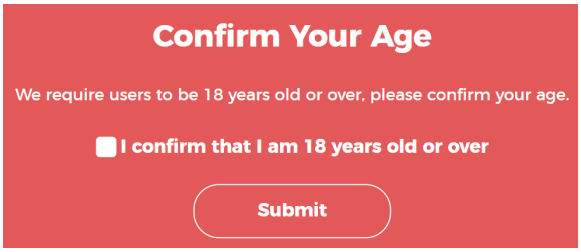


Figure 4: "Verification Theatre" Tick Box

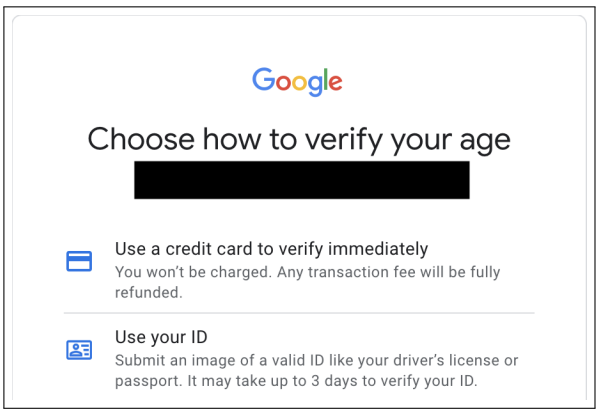


Figure 5: Google's Age Verification

verification product is the only one to be certified by the new Age Verification Regulator under the British Board of Film Classification (BBFC) age verification scheme [92]. Similar to Yoti, VerifyMyAge uses AI to estimate the age of the user [80] while AgeChecker.net and Jumio require a user to upload a selfie with their Government issued ID. AI is then utilised to determine the age of the user [37, 2].

Where some vendors accept credit cards only as a means of age verification, VeriMe allows age verification of customers who want to use a debit card [81]. This is achieved via vendors obtaining debit card information while VeriMe checks that the user's mobile number is registered to an adult over 18. AgeChecker.net, AgeChecked and VerifyMyAge also utilise a mobile number as a means of age verification [80, 2, 1]. Equifax, Experien and Trulioo rely on third-party database checks for age verification [19, 19, 78]. AgeChecked are the only vendor who claim to be able to do age verification through social media, but it is unclear how this method works in practice, and whether it is GDPR compliant. They also offer several other methods of verification [1]. Tencent [8] uses facial recognition to prevent children from entering their gaming platform.

Some commercial products estimate the age of a user from a facial biometric. Four of the most popular tools were tested by Jung *et al.* [38]. They found that none performed well when it came to age determination using a static image, making them unsuitable for online age verification. Yoti claims to have a 0.08% error rate and a Mean Absolute Error of 2.09 years [93]. Table 2 shows the range of commercial products in this space. Please note that only Business-to-Business commercial solutions which are available to purchase have been included in this table. Non-commercial age verification processes, such as the ones shown in Figures 4 and 5, are not included. Age verification, similar to authentication, also relies on: 'what you know', 'what you are', 'what you hold' and combinations of these. Because none of the commercial solutions utilize the first option, we have included a research-based solution (which was tested with over a thousand children) for the sake of completeness. This mechanism preserves privacy and is affordable, but is not effective because, while it could detect children, it also mis-classified a large percentage of adults.

We can now explain how solution types could be ranked on each of the three dimensions:

Table 2: Age Verification Products (details based on website check in June 2021)

Solution	Checks	Price
WHAT YOU KNOW		
Renaud and Maguire [61]	Knowledge and ability to identify photos of historical figures	N/A
WHAT YOU ARE		
Yoti [92]	Picture (AI)	25p per verification
Verify my Age [80]	Video (AI)	45p per verification (eBay)
WHAT YOU HOLD		
Yoti [92]	Government ID	25p per verification
	Phone Number	
Verify my Age [80]	Third Party Database Check	45p per verification
	Government ID	
	Credit Card Check	
	Phone Check	
VeriMe [81]	Phone Number Check (if using debit card)	Unknown
AgeChecker [2]	Third Party Database Check	$25 per month plus 50 cents per verified user
	Phone Number Check	
AgeChecked [1]	Driving Licence	Unknown
	Phone Number Check	
	Social Media	
	Payment Card	
	Address Search	
Trullioo [78]	Government ID	Unknown
	Third Party Database Check	
Melissa [46]	Address Check	Unknown
Equifax [19]	Third Party Database Check	Unknown
Experian [20]	Third Party Database Check	Unknown
WHAT YOU HOLD & ARE		
AgeChecker [2]	Selfie with ID (AI)	$25 per month plus 50 cents per verified user
Jumio [37]	Selfie with ID (AI)	Unknown
Tencent [8]	ID Card + Facial Recognition	Unknown

- **Effective & Inclusive:** While many age verification suppliers claim efficacy, children are likely to try a variety of ways of fooling them. For example, we used the online demo of one of the AI powered facial biometric mechanisms to test its efficacy (We do not identify this supplier because we have not been able to contact them to report this). It performed well with three adults in the over 25 age group. However, when we put a dog in front of the person's face, it estimated the age as 42-45 (see Figure 6 - we replicated this with a different dog). We contacted the company to tell them about this apparent vulnerability. They responded as follows: *We welcome and appreciate people helping us make our technology even better. Our age estimation AI simply looks at an image presented to it and provides an estimate in near real-time. While our demos will always provide a secure transfer of data, many don't have additional anti-spoofing layers. However, when Yoti's age estimation is implemented in real-world and online scenarios, we use a range of anti-spoofing techniques including face detection and liveness that prevent attempted attacks to trick the system. e.g. https://yoti.world/liveness.*

  Other mechanisms do a database lookup but a teenager could easily use a parent's name, or might even be named after a parent, impacting efficacy. A test for the person the phone is registered with might also turn up a false positive if the teenager's phone is registered in the parent's name. Government ID will indeed prove

age, but this either has to be scrutinised by a human so will also involve additional staff costs and processing delays, or by the use of pay-per-use AI techniques. Moreover, these techniques violate the user's privacy.

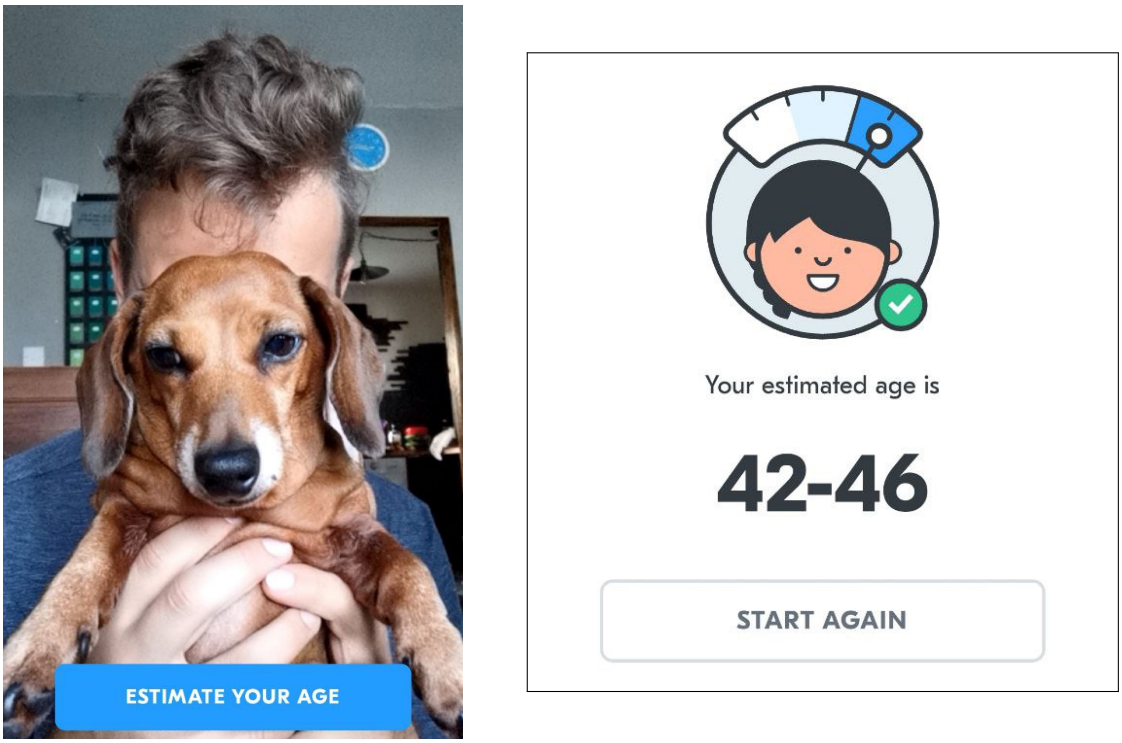


Figure 6: Fooling an Age Verification Mechanism with Ellie the dachshund

In addition to efficacy concerns, both Yar and Blake highlight the fact that age verification solutions using credit cards, passports or driving licenses exclude the economically disadvantaged [91, 7]. Those who either cannot gain access to a credit card due to limited financial resources, or those who choose not to have a credit card, will be excluded from accessing these services unless an alternative method of age verification is supported. The 2011 UK census shows that 24% of UK nationals do not have a passport and 15% do not have a driving licence [73]. Entering credit card, passport or driving license information into an adult-only website might also deter some privacy and security conscious adult users from accessing online services. The legitimate businesses trying to sell these products will suffer economically.

- **Affordable:** One of the main issues related to current commercial age verification products that could render them unsuitable is the cost to vendors. With people having to pay for each verification, costs could quickly become commercially infeasible for vendors selling low-cost products, such as beer or cigarettes. A number of online databases allow address lookup to confirm provided details, but the UK databases require payment (e.g., Royal Mail, the Electoral Roll and 192.com). Other countries probably have similar online services that offer lookups for a fee.

  Hence, for low value online services providing adult content or products, the current solutions' pricing models i.e., per verification, might well be unworkable for small and boutique businesses.

- **Privacy Respecting:** For adults looking to access online adult services or content discreetly and lawfully, entering credit card information, passport or driving license details or having their picture taken, are all privacy invasive. This is undesirable and risky.

  Yar [91] highlights the impact of the 2015 Ashley Madison breach and the concern that age verification providers might be targeted due to the sensitive and compromising information they may hold on users who have been verified through their service. Recently the rise in "extortionware" has seen people being targeted by hackers who have sought out sensitive information to extort money from them in return for ensuring the information is not leaked. This happened to an IT Director of a US company whose systems were infected with ransomware by a hacking group. In the process, hackers found a pornography collection on the IT Director's work device and posted a blog naming the Director and exposing their findings. The company did not respond to requests for comment and the blog post was removed by the hacking group, potentially implying that the ransom was paid [50].

4.3 Privacy Invasiveness

Very few of the commercial mechanisms preserve their users' privacy. These mechanisms use third party identity authentication mechanisms as a proxy for age verification. This is an overkill solution, which works very well for the vendors in terms of covering them from a legal perspective. Yet the user has to sacrifice their own privacy to use the service. The Ashley Madison breach made it clear what the fallout could be if usage of particular websites is leaked [4]. Ashley Madison facilitated adultery, which is not illegal, but many people consider such activities to be unacceptable and/or immoral.

Consider how age verification is achieved in the physical world. A person can walk into a bar and order a drink without identifying themselves, as long as they look old enough. If the vendor is unsure, they might ask to see proof, but no record is taken of such proof. On the Internet, it is hard to guarantee that identity documents will not be stored and potentially abused. This is why it is so important for people to be able to use adult-only services without risking identity theft or embarrassment. Moreover, children's identity data has to be protected even more than that of adults, even if they are potentially trying to access adult-only content (e.g. COPPA legislation in the USA [22] and GDPR in the European Union [35]).

4.4 Summary

Our review revealed that the majority of available age verification solutions are privacy-invasive, bringing the European Union's GDPR regulations and cyber security concerns into the picture, for both users and vendors. Information regarding a person's sex life or sexual orientation is classed as special category of data under the EU's GDPR regulation. This information could easily be revealed based on the websites people choose to use. Similarly, the California Privacy Rights Act (CPRA) 2020 defines government identifiers, sex life and sexual orientation as sensitive personal information

[82]. The sensitive nature of data that is potentially inferred or collected requires additional safeguards and security controls to protect it [35].

For any vendor buying a third-party age verification solution, there is a high level of due diligence required to ensure that the supply chain could not adversely impact their business. Biometric mechanisms are not privacy invasive when used to prove age and not to identify an individual but turn out not to be infallible, as we demonstrate.

5 Alternative Mechanisms

There is a clear requirement for more technical options to satisfy online age verification requirements, while preserving privacy. Combining the areas of age verification and deception detection may be a novel way of producing a privacy-preserving mechanism for verifying a user's age. By being able to detect, with a dependable accuracy, whether a user is deceitfully trying to access an adult service or buy an adult product, it could be judged with a high level of probability that the applicant is under 18.

5.1 Deception Detection

Deception detection techniques have been utilised for many years using a variety of physical cues and tools, such as lie-detector machines. It is claimed that an average person can detect deception with 54% accuracy while trained groups such as psychologists or interrogators, show approximately 60% accuracy [90]. The study of detection deception has moved on with the introduction of AI and the ability to detect deceit virtually rather than physically. Some of the techniques researched for detecting deception online include micro-expressions 'read' via the camera, pupil dilation, keyboard dynamics and mouse dynamics, all of which have varying degrees of accuracy[77, 48, 9, 47, 49].

The topic of deception detection is well researched and thoroughly critiqued. However, there is a lack of research with regards to detecting deception in children. There is also no evidence to suggest that deception detection has been used as a method for verifying age online.

5.2 Facial Cues

The most researched deception technique is the analysis of micro-expressions, which is based on the theories of psychologist Paul Ekman [15]. Micro-expressions are split-second facial cues which indicate emotional leakage and can be evidence of a concealed emotion [59]. Psychologists, investigators, and interrogators are turning to micro-expressions to detect whether someone is being deceitful, even marketeers are using facial expressions to enhance their market research [44, 21]. Facereader [21], for example, is a market research product that measures different variables, such as gender and age, as well as facial expressions while participants watch an advert. This information is analysed to determine how the participant reacted to the advert and ultimately how successful it may be in the wild.

Because micro-expressions are split-second facial cues, they can be difficult for the human eye to pick up. Ekman developed the Facial Action Coding Systems (FACS) which describes the criteria for observing and determining facial

muscle movements, or Action Units (AU) [13]. FACS has been used by technologists to develop a number of micro expression databases used in AI-powered deception detection systems [10]. A variety of technologies have been researched and developed to pick these up and analyse them. Wang *et al.* found that trained professionals only had a 47% accuracy rate in detecting micro-expressions [83] whereas Buhari *et al.* [10] claim that micro-expressions can be detected using AI with 65-80%.

Currently the most comprehensive micro-expression database is the Chinese Academy of Sciences Micro-Expression (CASME) II and it claims to have a 63.41% accuracy rate [83]. It has been researched and utilised by many in the psychology and AI domain but it does not seem to have been used to detect deception in children, or for age verification purposes.

5.3 Deception through keyboard dynamics

Because lying requires more cognitive processing than truth telling, Monaro *et al.* [47] found that they could detect a liar by means of the way they interacted with the computer keyboard with 92-94% accuracy. During their study, they posed unexpected text input questions for participants to answer. The unexpected questions put more cognitive strain on the liars, resulting in latency in their responses and a higher error rate. Monaro *et al.* [48], in previous research, also found the use of mouse dynamics and unexpected questions could detect liars with over 90% accuracy.

Given the increase in smartphone and tablet use, relying on mouse dynamics is not a future-proof solution. Similarly, many users will not interact with a traditional desktop keyboard but will instead use a soft keyboard on their smartphone or tablet. While deception detection has not been studied when soft keyboards are used, age-range prediction was investigated by Roy *et al.* [65]. Their study found that by getting youths under 18 and adults to type “Kolkata" into a smart phone, their machine learning model was able to predict the age group of the user with 80-82% accuracy. This was using keystroke dynamic motor behaviour and timing of typing as the main measurements.

5.4 Pupil dilation, blink rate and saccadic eye movement

Being able to detect deceit through physical cues in the eye has been researched by several psychologists and technologists in order to determine if technology can pick up subtle changes in pupil dilation, blink rate or saccadic eye movement. Pupil dilation was found by Trifiletti *et al.* [77] to be an accurate way of detecting deception. In their study, they found that pupil dilation greatly increased pre- and post- deceptive statements versus when a participant was telling the truth. This is one cue also advocated by Ekman, but cannot be used in isolation as a reliable indicator of deceit [16].

Similarly, Ekman believes that because lying requires more cognitive processing, blink rates decrease as a deceptive sign. This was investigated by Perelman *et al.* [56] and they did find that there was a difference in blink rate between liars and truth tellers. Borza *et al.* [9], using three different eye blink and facial databases (EyeBlink, Eyeblink 8 and Silesian), were unable to distinguish a correlation between blink rate and liars. However, when they developed a normalised blink rate deviation score, they were able to show which questions were answered truthfully or deceitfully.

Due to the fact blink rate decreases when more cognitive processing is required, even in truth tellers, it can be assumed that if the question is challenging or requires a thoughtful answer, this particular indicator might not deliver accurate deception cues, when used in isolation.

Borza *et al.* [9], in the same project, also investigated whether saccadic eye movements could be used as indicators of deception. Using the eye movement criteria set out by Ekman's FACS and the Silesian database, they were unable to distinguish any pattern related to saccadic eye movement and deceit.

5.5 Applications and Criticisms

Using techniques to detect micro-expressions in order to detect deception was trialled on a large scale recently in Europe through an AI product called iBorderCtrl. It was trialled in three European countries land borders, Greece, Latvia and Hungary, and it aimed to detect travellers who were lying about their identity or reason for travel. The project attracted significant attention and was heavily criticised by researchers and ethics groups who argued the system was not ready for *in vivo* testing [39].

Relying on Ekman's micro-expression theories, the system measured micro-expressions of travellers to determine whether the traveller showed signs that they were concealing their inner state. If the system flagged a traveller, they would be taken for further questioning by appropriate border staff [39]. With the system utilising AI, the data set used to train the model has been questioned. Sanchez and Dencik [66] highlight the fact that the iBorderCtrl developers used 32 participants to tell truthful and deceptive statements while video segments were analysed to determine a total of 38 cues labelled truthful or deceptive. Of the 32 participants, 69% were male and 69% were of White European background, calling into question the diversity of the participants used to train the AI model.

Micro-expressions, and their ability to be used for deception detection, has come under heavy fire from a variety of researchers. Lisa Feldman-Barrett [23] has criticised Ekman's work stating that Ekman 'primed' his subjects while developing his micro-expression theories by offering them a closed choice of options to classify expressions. When she repeated his experiments with open choices, she found that recognition of emotions became little better than chance. Similarly, Holmes [33] found that micro-expressions can be "squelched" by a deliberate macro-expression such as a Non-Duchenne smile [94], which would make it difficult to detect a deceptive micro-expression.

However, there remains an argument for utilising AI to detect deception. Kleinberg *et al.* found AI to be significantly more effective at detecting deceit than humans. The AI system that they tested had an overall accuracy score of 69% but when humans were asked to overrule judgements they felt the system did not correctly identify, the accuracy levels were reduced to chance [41].

6 Discussion

Returning to the initial research questions set out at the start of this paper:

RQ1: *To what extent do online age verification solutions exhibit the three primary dimensions enumerated in Section 2.3?*

A range of solutions exist, as discussed in Sections 4.1 and 4.2. There are severe limitations in terms of efficacy. Where the solution is effective, it is almost always extremely privacy invasive. Where the solution *is* privacy preserving, it tends to be ineffective. Currently, the most utilised method for age verification is a tick box for the user to confirm they are over 18 (e.g., Figure 4). Other common methods include taking a photo of the user and using AI to determine the user's age. These are not infallible, as we show in Figure 6.

Privacy invasive mechanisms dominate, including taking credit card details, requiring personal information to be provided to enable third-party database verification or having a phone number verified (e.g., Figure 5).

Considering the challenges on each of the dimensions enumerated in Section 2.3, we see that the available solutions generally fail on at least one of the dimensions, with the majority invading privacy.

RQ2: *What other mechanisms could potentially be used to effect age verification?*

Section 5 reviews a number of directions for future research. In particular, deception detection demonstrates promise. The main methods being researched in other domains of deception detection are the ability to detect deception through micro-expressions, blink rate and keyboard and mouse dynamics. There is significant research and development in this area that could inform its use in age verification.

6.1 Reflection and Future Work

Combining the current research areas of age verification and deception detection could provide a novel, privacy preserving approach to the industry problem of preventing youths accessing adults services or products online.

In order to determine whether a user is pretending to be over 18, and trying to access adult services and content online, it is proposed that they be asked to answer free-text questions as part of an age verification process. Using the built-in device camera and keyboard, a machine learning model will take both the camera and keyboard input and evaluate whether the user's behaviour is abnormal, concluding with a deception-likelihood estimate. If the user is deemed to be deceptive, it will be assumed that they are under 18 and trying to conceal this fact.

With respect to the proposed future directions for research, we do not know how inclusive the micro-expression detection will prove to be across all members of the population, including minorities, especially since other mechanisms have failed in this respect [18]. Yet, there is still some disagreement between academics such as Feldman-Barrett [23] and Ekman [16] about whether micro-expressions can be used to signal deception attempts. This is clearly an area calling out for rigorous investigation.

Rigorous age verification mechanisms might well constitute an unacceptable barrier to customers, turning them away altogether because they create too much friction. Mechanisms that are easy to traverse might not be effective in preventing children from accessing the service. The company might then have to pay a fine, which will also affect their bottom line. There is likely to be a sweet spot that has yet to be identified in this space.

6.2 Limitations

There has been increasing use of facial recognition for a wide range of purposes over the last few years. Law enforcement has been a particularly enthusiastic adopter [63]. Just recently, official bodies such as the Information Commissioner in the UK have expressed grave concerns about its use [5]. We should note that the kind of biometric we propose is not the same as these, which compare a face to a stored database of faces. We do not need to store any of the images. We will only use them to help us to to estimate the adulthood of an end user. We will process the face biometric to make a judgement, and then delete all artefacts gathered for processing purposes. We will also make it very clear to the user, *before* they allow us to access the camera to see their face, that we will be processing their face algorithmically, and assure them that we will not be storing it on any of our databases, to ensure that we are GDPR compliant [35].

7 Conclusion

This paper presents a snapshot of the online age verification arena. We reviewed the current solutions, both research and commercial, and highlighted the general privacy invasiveness of most. We suggest directions for the development of more privacy-protective age verification mechanisms.

We carried out this literature review to provide a snapshot of the state of play related to age verification. We aimed to trigger a discourse into whether it is feasible to come up with a solution that satisfies all dimensions, marked as the "ideal solution" in Figure 1. If not, how do we decide which sector within this three dimensional space we should aim to satisfy? Which is the most important dimension and how do we rank them? There is certainly a tension that needs to be resolved. We also welcome inputs from other researchers related to the viability of the suggested mechanisms outlined in Section 6, in crafting a better age verification solution.

References

[1] AgeChecked. Age Checked, 2021. Retrieved 16/6/21 from: `https://www.agechecked.com/online-verification-solutions/`.

[2] AgeChecker.net. AgeChecker.net, 2021. Retrieved 29/05/21 from: `https://agechecker.net/`.

[3] C. Baraniuk. Ashley Madison: Leaked accounts fallout deepens, 2015. Retrieved 18 June 2021 from: `https://www.bbc.co.uk/news/technology-34002915`.

[4] C. Baraniuk. Ashley madison: Leaked accounts fallout deepens, 2015. Retrieved 15 August 2021 from: https://www.bbc.co.uk/news/technology-34002915.

[5] BBC. ICO watchdog 'deeply concerned' over live facial recognition, 2021. Retrieved 18 June 2021 from: https://www.bbc.co.uk/news/technology-57504717.

[6] BBC News. Porn blocker 'missing' from Online Safety Bill prompts concern, 2021. Retrieved 18/05/21 from: https://www.bbc.co.uk/news/technology-57143746.

[7] P. Blake. Age verification for online porn: more harm than good? *Porn Studies*, 6(2):228–237, 2019.

[8] M. Borak. Kids are trying to outsmart Tencent's facial recognition system by pretending to be their grandads, 2018. Retrieved 17 June from: https://www.scmp.com/abacus/tech/article/3029027/kids-are-trying-outsmart-tencents-facial-recognition-system-pretending.

[9] D. Borza, R. Itu, and R. Danescu. In the eye of the deceiver: Analyzing eye movements as a cue to deception. *Journal of Imaging*, 4(10):120, 2018.

[10] A. M. Buhari, C.-P. Ooi, V. M. Baskaran, R. C. Phan, K. Wong, and W.-H. Tan. FACS-Based Graph Features for Real-Time Micro-Expression Recognition. *Journal of Imaging*, 6(12):130, 2020.

[11] T. Byron. Safer children in a digital world: The report of the Byron Review: Be safe, be aware, have fun, 2008. Retrieved 31 May 2020, from https://childcentre.info.

[12] S. Colbert, L. Thornton, and R. Richmond. Content analysis of websites selling alcohol online in Australia. *Drug and Alcohol Review*, 39(2):162–169, 2020.

[13] A. K. Davison, W. Merghani, and M. H. Yap. Objective classes for micro-facial expression recognition. *Journal of Imaging*, 4(10):119, 2018.

[14] S. Dunn and A. Petricone-Westwood. More than 'Revenge Porn' Civil Remedies for the Nonconsensual Distribution of Intimate Images. In S. Dunn and A. Petricone-Westwood, editors, *38th Annual Civil Litigation Conference*, volume 16, 2018.

[15] P. Ekman. Microexpressions, 2021. Retrieved 10/06/21 from: https://www.paulekman.com/resources/micro-expressions.

[16] P. Ekman. Signs of Lying, 2021. Retrieved 15/06/21 from: https://www.paulekman.com/blog/signs-of-lying/.

[17] engadget. TikTok's older users are being blocked after it introduced age checks, 2019. Accessed: 28/06/2021 https://www.engadget.com/2019-03-01-tiktok-age-checks-blocked-users.html.

[18] A. Engler. The Reason Auditors Are Struggling To Hold AI Accountable, 2021. Retrieved 28 January 2021 from: http://www.thelowdownblog.com/2021/01/the-reason-auditors-are-struggling-to.html Jan. 27.

[19] Equifax. Equifax Age Verification, 2021. Retrieved 29/05/21 from: https://www.equifax.co.uk/business/age-verification/en_gb/.

[20] Experien. Experien Age Verification, 2021. Retrieved 29/05/21 from: https://www.experian.co.uk/business/identity-fraud/validation/age-verification/.

[21] Facereader. Facereader Online, 2021. Accessed: 28/06/2021 https://www.facereader-online.com/f.

[22] Federal Trade Commission. Complying with COPPA: Frequently Asked Questions, 2021. Retrieved 21/05/21 from: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0.

[23] L. Feldman-Barrett. *How Emotions Are Made: The Secret Life of The Brain*. Houghton Mifflin Harcourt, 2017.

[24] S. Fischer. Kids' daily screen time surges during coronavirus, 2020. Retrieved 20 June 20201 from: https://www.axios.com/kids-screen-time-coronavirus-562073f6-0638-47f2-8ea3-4f8781d6b31b.html.

[25] S. M. Gaiha, L. K. Lempert, and B. Halpern-Felsher. Underage Youth and Young Adult e-Cigarette Use and Access Before and During the Coronavirus Disease 2019 Pandemic. *JAMA Network Open*, 3(12):e2027572–e2027572, 2020.

[26] K. Geldenhuys. The link between teenage alcohol abuse, sexting & suicide. *Servamus Community-based Safety and Security Magazine*, 110(6):14–18, 2017.

[27] F. Gilbert. Age verification as a shield for minors on the internet: A quixotic search. *Shidler JL Com. & Tech.*, 5:1, 2008.

[28] GOV.UK. Digital Economy Bill receives Royal Assent, 2017. Retrieved 3/06/21 from: https://www.gov.uk/government/news/digital-economy-bill-receives-royal-assent.

[29] GOV.UK. Age Verification for Online Pornography to Begin in July, 2019. Retrieved 16/06/21 from: https://www.gov.uk/government/news/age-verification-for-online-pornography-to-begin-in-july.

[30] GOV.UK. Draft Online Safety Bill, 2021. Retrieved 12/06/21 from: https://www.gov.uk/government/publications/draft-online-safety-bill.

[31] GOV.UK. Government calls for age verification on alcohol sales, 2021. Retrieved 21/05/21 from: https://www.gov.uk/government/publications/age-verification-technology-in-alcohol-sales-regulatory-sandbox/call-for-proposals.

[32] G. Hartley and M. Karinch. *I Can Read You Like a Book: How to Spot the Messages and Emotions People Are Really Sending with Their Body Language*. Career Press, Franklin Lakes, USA, 2007.

[33] M. Holmes. National security behavioral detection: a typography of strategies, costs, and benefits. *Journal of Transportation Security*, 4(4):361–374, 2011.

[34] C. Hughes. *Six-Minute X-Ray: Rapid Behavior Profiling*. Evergreen Press, Delaware, USA, 2020.

[35] Information Commissioners Office. Special Category Data, 2021. Retrieved 14/06/21 from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

[36] ISO. Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts. ISO 9241-11:2018, 2018.

[37] Jumio. Jumio, 2021. Retrieved 16/6/21 from: https://www.jumio.com/use-case/age-verification/.

[38] S.-G. Jung, J. An, H. Kwak, J. Salminen, and B. Jansen. Assessing the accuracy of four popular face recognition tools for inferring gender, age, and race. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 12, 2018.

[39] L. M. Jupe and D. A. Keatley. Airport artificial intelligence can detect deception: or am i lying? *Security Journal*, 33(4):622–635, 2020.

[40] K. S. Khan, R. Kunz, J. Kleijnen, and G. Antes. Five steps to conducting a systematic review. *Journal of the Royal Society of Medicine*, 96(3):118–121, 2003.

[41] B. Kleinberg and B. Verschuere. How humans impair automated deception detection performance. *Acta Psychologica*, 213:103250, 2021.

[42] P. Kumar, R. K. Rao, and N. H. Reddy. Sustained uptake of LPG as cleaner cooking fuel in rural India: Role of affordability, accessibility, and awareness. *World Development Perspectives*, 4:33–37, 2016.

[43] S. Livingstone, J. Carr, and J. Byrne. One in three: Internet governance and children's rights, 2016. UNICEF. Office of Research-Innocenti.

[44] D. Luciew, J. Mulkern, and R. Punako. Finding the truth: interview and interrogation training simulations. In *Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)*, 2011.

[45] E. Martellozzo, A. Monaghan, J. R. Adler, J. Davidson, R. Leyva, and M. A. Horvath. "I wasn't sure it was normal to watch it..." A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people, 2016. Middlesex University, NSPCC, OCC https://www.mdx.ac.uk/__data/assets/pdf_file/0021/223266/MDX-NSPCC-OCC-pornography-report.pdf.

[46] Mellisa. Mellisa, 2021. Retrieved 16/6/21 from: https://www.melissa.com/age-verification/.

[47] M. Monaro, C. Galante, R. Spolaor, Q. Q. Li, L. Gamberini, M. Conti, and G. Sartori. Covert lie detection using keyboard dynamics. *Scientific Reports*, 8(1):1–10, 2018.

[48] M. Monaro, L. Gamberini, and G. Sartori. The detection of faked identity using unexpected questions and mouse dynamics. *PloS One*, 12(5):e0177851, 2017.

[49] T. Nahari, O. Lancry-Dayan, G. Ben-Shakhar, and Y. Pertzov. Detecting concealed familiarity using eye movements: The role of task demands. *Cognitive Research: Principles and Implications*, 4(1):1–16, 2019.

[50] B. News. 'We have your porn collection': The rise of extortionware, 2021. Retrieved 10/06/21 from: https://www.bbc.co.uk/news/technology-56570862.

[51] Newstalk. British teenager who idolised serial killer found guilty of two murders, 2016. Accessed 26 June 2021 https://www.newstalk.com/news/james-fairweather-serial-killer-britain-guilty-yorkshire-ripper-murders-601896.

[52] NSPCC. Online safety during coronavirus, 2021. Retrieved 12/06/21 from: https://learning.nspcc.org.uk/news/covid/online-safety-during-coronavirus.

[53] Ofcom. Ofcom report on Internet safety measures. Strategies of parental protection for children online, 2015. Accessed: Jan. 12, 2018 https://www.ofcom.org.uk/__data/assets/pdf_file/0020/31754/Fourth-Internet-safety-report.pdf.

[54] Ofcom. Childrens Code, 2020. Accessed: 19/06/2021 https://ico.org.uk/childrenscode.

[55] Ofcom. Parents' rising concern over children online, 2020. Accessed 16 June 2021 https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020.

[56] B. S. Perelman. Detecting deception via eyeblink frequency modulation. *PeerJ*, 2:e260, 2014.

[57] N. PERLROTH. Verifying Ages Online Is a Daunting Task, Even for Experts, 2012. Retrieved 15/08/21 from: https://web.archive.org/web/20180131002202/https://www.nytimes.com/2012/06/18/technology/verifying-ages-online-is-a-daunting-task-even-for-experts.html.

[58] J. Peter and P. M. Valkenburg. Adolescents' exposure to sexually explicit internet material and notions of women as sex objects: Assessing causality and underlying processes. *Journal of Communication*, 59(3):407–433, 2009.

[59] S. Porter, L. Ten Brinke, and B. Wallace. Secrets and lies: Involuntary leakage in deceptive facial expressions as a function of emotional intensity. *Journal of Nonverbal Behavior*, 36(1):23–37, 2012.

[60] A. Quadara, A. El-Murr, and J. Latham. The effects of pornography on children and young people. *Australian Institute of Family Studies: Melbourne*, 2017.

[61] K. Renaud and J. Maguire. Regulating access to adult content (with privacy preservation). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 4019–4028, 2015.

[62] K. Renaud and S. Prior. The "three M's" counter-measures to children's risky online behaviors: mentor, mitigate and monitor. *Information & Computer Security*, 29(3):526–557, 2021. https://doi.org/10.1108/ICS-07-2020-0115.

[63] K. Ringrose. Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns. *Va. L. Rev. Online*, 105:57, 2019.

[64] S. Rouse and J. Ford. *Understanding Body Language: How to Decode Nonverbal Communication in Life, Love, and Work*. Rockbridhge Press, California, USA, 2021.

[65] S. Roy, U. Roy, and D. Sinha. The probability of predicting personality traits by the way user types on touch screen. *Innovations in Systems and Software Engineering*, 15(1):27–34, 2019.

[66] J. Sánchez-Monedero and L. Dencik. The politics of deceptive borders:'biomarkers of deceit'and the case of iBorderCtrl. *Information, Communication & Society*, pages 1–18, 2020.

[67] S. J. Schiff, A. Kechter, K. A. Simpson, R. C. Ceasar, J. L. Braymiller, and J. L. Barrington-Trimis. Accessing vaping products when underage: A qualitative study of young adults in southern california. *Nicotine & Tobacco Research : Official Journal of the Society for Research on Nicotine and Tobacco*, 2021.

[68] J. Schreyögg, M. Bäumler, and R. Busse. Balancing adoption and affordability of medical devices in Europe. *Health Policy*, 92(2-3):218–224, 2009.

[69] R. Shambare. The adoption of whatsapp: breaking the vicious cycle of technological poverty in south africa. *Journal of Economics and Behavioral Studies*, 6(7):542–550, 2014.

[70] V. C. Strasburger, H. Zimmerman, J. R. Temple, and S. Madigan. Teenagers, sexting, and the law. *Pediatrics*, 143(5):e20183183, 2019.

[71] Tech Crunch. TikTok will recheck the age of every user in Italy after DPA order, 2021. Accessed: 28/06/2021 `https://techcrunch.com/2021/02/03/tiktok-will-recheck-the-age-of-every-user-in-italy-after-dpa-order/?guccounter=1`.

[72] The Guardian. UK government faces action over lack of age checks on adult sites, 2021. Retrieved 15/05/21 from: `https://www.theguardian.com/society/2021/may/05/uk-government-faces-action-over-lack-of-age-checks-on-pornography-websites`.

[73] The Independent. By forcing voters show their ID, the Government has found another way to disenfranchise the poor, 2016. Retrieved 10/06/21 from: `https://www.independent.co.uk/voices/voter-id-passport-drivers-license-disenfranchise-poor-a7497801.html`.

[74] D. S. Thomas. Cyberspace pornography: Problems with enforcement. *Internet Research*, 7(3):201–207, 1997.

[75] R. Thompson. Teen girls' online practices with peers and close friends: implications for cybersafety policy. *Australian Educational Computing*, 31(2):1–16, 2016.

[76] J. Torluemke and C. Kim. NortonLifeLock Study: Majority of Parents Say Their Kids' Screen Time Has Skyrocketed During the COVID-19 Pandemic, 2020. Retrieved 20 June 20201 from: `https://investor.nortonlifelock.com/About/Investors/press-releases/press-release-details/2020/NortonLifeLock-Study-Majority-of-Parents-Say-Their-Kids-Screen-Time-Has-Skyrocketed-During-the-COVID-19-Pandemic/default.aspx`.

[77] E. Trifiletti, S. D'Ascenzo, L. Lugli, V. M. Cocco, G. A. Di Bernardo, C. Iani, S. Rubichi, R. Nicoletti, and L. Vezzali. Truth and lies in your eyes: Pupil dilation of White participants in truthful and deceptive responses to White and Black partners. *Plos One*, 15(10):e0239512, 2020.

[78] Trulioo. Trulioo, 2021. Retrieved 16/6/21 from: https://www.trulioo.com/.

[79] UK Safer Internet Centre. Age Restrictions on Social Media, 2018. Accessed: 28/06/2021 https://www.saferinternet.org.uk/blog/age-restrictions-social-media-services.

[80] VerifyMyAge. VerifyMyAge, 2021. Retrieved 29/05/21 from: https://www.verifymyage.co.uk/.

[81] VeriMe. VeriMe, 2021. Retrieved 29/05/21 from: https://verime.net/.

[82] T. Wallace. What is CPRA California Privacy Rights Act Basics Overview, 2021. Retrieved 21 July 2021, from https://www.the-future-of-commerce.com/2021/05/27/what-is-cpra-california-privacy-rights-act-basics-overview/.

[83] Y. Wang, J. See, Y.-H. Oh, R. C.-W. Phan, Y. Rahulamathavan, H.-C. Ling, S.-W. Tan, and X. Li. Effective recognition of facial micro-expressions with video motion magnification. *Multimedia Tools and Applications*, 76(20):21665–21690, 2017.

[84] R. S. Williams, J. Derrick, A. K. Liebman, K. LaFleur, and K. M. Ribisl. Content analysis of age verification, purchase and delivery methods of internet e-cigarette vendors, 2013 and 2014. *Tobacco Control*, 27(3):287–293, 2018.

[85] R. S. Williams, J. Derrick, and K. M. Ribisl. Electronic cigarette sales to minors via the internet. *JAMA Pediatrics*, 169(3):e1563–e1563, 2015.

[86] R. S. Williams and J. C. Derrick. Internet little cigar and cigarillo vendors: surveillance of sales and marketing practices via website content analysis. *Preventive Medicine*, 109:51–57, 2018.

[87] R. S. Williams and K. M. Ribisl. Internet alcohol sales to minors. *Archives of Pediatrics & Adolescent Medicine*, 166(9):808–813, 2012.

[88] G. M. Winters, L. E. Kaylor, and E. L. Jeglic. Sexual offenders contacting children online: an examination of transcripts of sexual grooming. *Journal of Sexual Aggression*, 23(1):62–76, 2017.

[89] N. Wood. Charlotte's accessible web: how West Australian children and adolescents can access e-cigarettes online. *Australian and New Zealand Journal of Public Health*, 45(1):81–82, 2021.

[90] M. H. Yap, H. Ugail, and R. Zwiggelaar. Facial behavioral analysis: A case study in deception detection. *British Journal of Applied Science and Technology*, 4(10):1485–1496, 2014.

[91] M. Yar. Protecting children from Internet pornography? A critical assessment of statutory age verification and its enforcement in the UK. *Policing: An International Journal*, 43(1):183–197, 2019.

[92] Yoti. Yoti, 2021. Retrieved 29/05/21 from: https://www.yoti.com/.

[93] Yoti. Yoti Age Scan, 2021. Retrieved 14/06/21 from: https://www.yoti.com/wp-content/uploads/Yoti-age-estimation-White-Paper-May-2021.pdf.

[94] M. Zloteanu. *Reconsidering Facial Expressions and Deception Detection*. FEELab Science Books, 2020.

A Appendix A

EXHIBIT E

Onion Routing for Anonymous and Private Internet Connections

David Goldschlag* Michael Reed† Paul Syverson†

January 28, 1999

1 Introduction

Preserving privacy means not only hiding the content of messages, but also hiding who is talking to whom (traffic analysis). Much like a physical envelope, the simple application of cryptography within a packet-switched network hides the messages being sent, but can reveal who is talking to whom, and how often. Onion Routing is a general purpose infrastructure for private communication over a public network [8, 9, 4]. It provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. The connections are bidirectional, near real-time, and can be used for both connection-based and connectionless traffic. Onion Routing interfaces with off the shelf software and systems through specialized proxies, making it easy to integrate into existing systems. Prototypes have been running since July 1997. As of this article's publication, the prototype network is processing more than 1 million Web connections per month from more than six thousand IP addresses in twenty countries and in all six main top level domains. [7]

Onion Routing operates by dynamically building anonymous connections within a network of real-time Chaum Mixes [3]. A Mix is a store and forward device that accepts a number of fixed-length messages from numerous sources, performs cryptographic transformations on the messages, and then forwards the messages to the next destination in a random order. A single Mix makes tracking of a particular message either by specific bit-pattern, size, or ordering with respect to other messages difficult. By routing through numerous Mixes in the network, determining who is talking to whom becomes even more difficult. Onion Routing's network of core onion-routers (Mixes) is distributed, fault-tolerant, and under the control of multiple administrative domains, so no single onion-router can bring down the network or compromise a user's privacy, and cooperation between compromised onion-routers is thereby confounded.

*Divx, Herndon, VA USA, david.goldschlag@divx.com

†Center for High Assurance Computer Systems, Naval Research Laboratory, Washington, DC USA, {reed, syverson}@itd.nrl.navy.mil

2 Application Support via Proxies

Onion Routing can be used with applications that are proxy-aware, as well as several non-proxy-aware applications, without modification to the applications. Currently supported protocols include HTTP, FTP, SMTP, rlogin, telnet, NNTP, finger, whois, and raw sockets. Proxies are under development for Socks5, DNS, NFS, IRC, HTTPS, SSH, and Virtual Private Networks (VPNs). A proxy has three logical layers: an optional application specific privacy filter that sanitizes the data streams; an application specific proxy that translates the data streams into an application independent format accepted by the Onion Routing network; and lastly, an onion proxy that builds and manages the anonymous connections. Because it builds and manages the anonymous connections, the onion proxy is the most trusted component in the system. Likewise, to build onions and hence define routes the onion proxy must know enough of the topology and link state of the network, the public certificates of nodes in the network, and the exit policies of nodes in the network. This information is distributed securely within the network automatically as new nodes come on-line or as the information changes.

3 Moving Data through the Network

Onion Routing's anonymous connections are protocol independent and exist in three phases: connection setup, data movement, and connection tear-down. Setup begins when the initiator creates an onion, which defines the path of the connection through the network. An onion is a (recursively) layered data structure that specifies properties of the connection at each point along the route, e.g. cryptographic control information such as the different symmetric cryptographic algorithms and keys used during the data movement phase. Each onion router along the route uses its public key to decrypt the entire onion that it receives. This operation exposes the cryptographic control information, the identity of the next onion router, and the embedded onion. The onion router pads the embedded onion to maintain a fixed size, and sends it to the next onion router. After the connection is established, data can be sent in both directions. Data from the initiator is repeatedly pre-encrypted using the algorithms and keys that were specified in the onion. As data moves through the anonymous connection, each onion-router removes one layer of encryption as defined by the cryptographic control information in the onion defining the route, so the data arrives as plaintext at the recipient. This layering occurs in the reverse order (using different algorithms and keys) for data moving backward. Connection tear-down can be initiated by either end, or in the middle if needed.

All information (onions, data, and network control) are sent through the Onion Routing network in uniform-sized cells. All cells arriving at an onion-router within a fixed time interval are mixed together to reduce correlation by network insiders. Likewise, the long-standing connections between onion-routers can be padded and bandwidth-limited to foil external observers. An Onion looks

different to each onion-router along a connection because of the layered public-key cryptography. Similarly, the layering of symmetric cryptography over the data phase cells makes them appear different to each onion-router. This design resists traffic analysis more effectively than any other deployed mechanisms for Internet communication.

4 Overhead

Onion Routing's overhead is relatively small. Connection setup overhead is typically much less than one second and appears to be no more noticeable than other delays associated with normal web connection setup on the Internet. Computationally expensive public-key cryptography is used only during this connection setup phase. Also, because public key decryption is much more expensive than encryption, the public key burden is mainly placed upon the onion routers themselves, where dedicated hardware acceleration can be justified. The data movement phase uses only secret-key (symmetric) cryptography, which is much faster. Furthermore, since the symmetric encryption can be pipelined, data throughput can be made as fast as ordinary link or end-to-end encryption. Data latency is affected by the number of onion-routers along the connection and can vary with route length and the duration of the Mix cycles.

5 Network Architectures that Shift Trust

Proxies, onion-routers, and other components can be run in a variety of distributed configurations. This allows Onion Routing to mesh well with a wide variety of operational and policy environments. At one extreme, proxies can run remotely. If a user makes a secure connection (e.g., encrytped or withing a firewall) to a trusted remote proxy, Onion Routing's protection can be utilized without installing any software or inducing local computational overhead. At the other extreme, all trusted components can run locally, providing maximum protection of anonymity and privacy against non-local components, even those participating in a connection. In between these two extremes are multiple configurations of proxies and onion routers, running on enclave firewalls or at ISPs.

By shifting trust in this way, Onion Routing can also complement other services like the Anonymizer [1] and LPWA [6]. The Anonymizer uses a central, trusted intermediary to provide sender anonymity (i.e., hide the identity of the sender from the receiver). If Onion Routing is used for privacy, an Anonymizer can run as a filtering proxy on the user's desktop (or the enclave firewall, or the user's ISP) to add sender anonymity. Security is improved because the filtering executes on a machine the user trusts, and communication leaving that machine will resist traffic analysis. Such security in depth removes the central point of failure for network traffic anonymity. LPWA provides various psuedonymy-based services (described elsewhere in this issue). Like Onion Routing it is

designed to handle email in addition to HTTP. And, like Onion Routing, it can be configured so that trusted functions are performed at various locations [2]. However, communication between and from these points is not itself anonymous or resistant to traffic analysis. This makes LPWA and Onion Routing especially natural complements.

6 Extensions

A natural extension to Onion Routing is the introduction of reply onions. Reply onions allow connections to be made back to an anonymous sender through the Onion Routing network long after the original connection existed. Reply Onions could be used to send anonymous replies in response to a previously received anonymous email. They could also enable novel applications such as anonymous publishing (anonymous URLs) similar to the Rewebber project [5].

7 Conclusion

In summary, Onion Routing is a traffic analysis resistant infrastructure that is easily accessible, has low overhead, can protect a wide variety of applications, and is flexible enough to adapt to various network environments and security needs. The system is highly extensible, allowing for additional symmetric cryptographic algorithms, proxies, or routing algorithms with only minor modifications to the existing code base. Instructions for accessing the Onion Routing network can be found on our web page along with additional background, pointers to publications, and contact information [7].

References

[1] The Anonymizer. `http://www.anonymizer.com/`

[2] D. Bleichenbacher, E. Gabber, P. Gibbons, Y. Matias, and A. Mayer. "On Secure and Pseudonymous Client-Relationships with Multiple Servers", to appear in *Proc.* 3^{rd} *USENIX Electronic Commerce Workshop* , August 1998.

[3] D. Chaum. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, v. 24, n. 2, Feb. 1981, pp. 84-88.

[4] D. Goldschlag, M. Reed, P. Syverson. "Hiding Routing Information", in *Information Hiding*, R. Anderson, ed., LNCS vol. 1174, Springer-Verlag, 1996, pp. 137–150.

[5] I. Goldberg and D. Wagner. "TAZ Servers and the Rewebber Network: Enabling Anonymous Publishing on the World Wide Web", *First Monday*, vol. 3 no. 4, April 1998.

[6] The Lucent Personalized Web Assistant. `http://lpwa.com/`

[7] The Onion Routing Home Page. `http://www.onion-router.net/`

Conference:

[8] M. Reed, P. Syverson, and D. Goldschlag. "Anonymous Connections and Onion Routing", *IEEE Journal on Selected Areas in Communications*, vol. 16 no. 4, May 1998, pp. 482–494.

[9] P. Syverson, M. Reed, and D. Goldschlag. "Private Web Browsing", *Journal of Computer Security*, vol. 5 no. 3, 1997, pp. 237–248.